



FRANCE STRATÉGIE
ÉVALUER. ANTICIPER. DÉBATTRE. PROPOSER.

Les enjeux des blockchains

RAPPORT

JUIN
2018

Rapport du groupe de travail présidé par Joëlle TOLEDANO



LES ENJEUX DES BLOCKCHAINS

Présidente du groupe de travail

Joëlle Toledano

Rapporteur

Lionel Janin





AVANT-PROPOS

La technique de la blockchain permet de transmettre des informations, regroupées en « chaînes de blocs », avec un degré élevé de sécurité, grâce à des méthodes de cryptage et à des protocoles de transmission. Elle permet d'assurer leur identité dans une série de points distincts : les nœuds d'un réseau. Pourquoi un tel engouement pour un procédé qui aurait pu n'intéresser que quelques spécialistes ?

Plusieurs facteurs se conjuguent pour l'expliquer : la promesse libertarienne d'une gestion très sûre de l'information sans qu'une autorité centrale en soit garante ; la perspective plus terre à terre de l'efficacité de l'utilisation de cette technique dans de nombreux domaines du quotidien, des transactions en ligne à l'exécution automatique de contrats ; enfin et surtout, le lien qui s'est établi entre blockchain et émission et usage de cryptomonnaies, circulant dans le réseau, et émises, le plus souvent, sur la base de la démonstration d'un investissement informatique permettant de résoudre un problème de cryptographie.

Ces cryptomonnaies ont fait l'objet d'un immense intérêt spéculatif, qui s'est cristallisé sur la première d'entre elles, le bitcoin, bientôt suivi de nombreuses autres. Des sommes importantes ont été réunies dans des levées de fonds – les ICO – parfois de grande taille, réalisées rapidement, sur la base de documentations très éloignées de celles prévalant dans le monde des actifs financiers ordinaires. Autorités bancaires et de marché se sont emparées de la question, et tentent de trouver un équilibre entre l'encouragement à l'usage de la technique au nom des perspectives de progrès qu'elle annonce, et régulation visant à protéger acteurs économiques y ayant recours et épargnants investissant dans les cryptomonnaies ou les ICO.

France Stratégie a souhaité faire un point d'étape sur la question. C'est l'objet de ce rapport, rédigé sous l'autorité de Joëlle Toledano, et qui a bénéficié de l'apport d'un groupe de travail réunissant un large champ d'expertises. Il décrit les grandes lignes de la technique et de ses principaux usages. Il prend position sur le lien, qu'il présente comme fort, entre usage large de la technique et recours aux cryptomonnaies : sujet très débattu. Il formule un certain nombre de propositions à

destination des pouvoirs publics. Une annexe décrit les origines libertariennes de la fascination originelle pour cette technique ; une autre fait le point sur certaines des principales questions juridiques qu'elle pose : caractère probant des transactions utilisant la technique, nature et régime des actifs que sont les cryptomonnaies.

Gilles de Margerie

Commissaire général de France Stratégie



PRÉFACE

Hier encore inconnue, mais déjà portée par le phénomène bitcoin, la blockchain est aujourd'hui à l'agenda de tous les décideurs. De fait, cette technologie numérique qui permet de transmettre des données de manière décentralisée, sécurisée, transparente et sans intermédiaire apparaît riche en potentialités. Certains y voient l'innovation disruptive qui va bouleverser la plupart des secteurs économiques, les plus optimistes allant jusqu'à annoncer l'entrée dans une ère de l'efficacité et de la confiance partagée. D'autres au contraire s'inquiètent d'une technologie à la réputation sulfureuse, présentant autant de lacunes que de risques : à leurs yeux, ces « chaînes de blocs » seraient à la fois l'objet d'une fascination spéculative – à l'image de la bulle internet du début des années 2000 – et le cheval de Troie de la criminalité.

Par peur de rater le coche, les secteurs de la banque et de l'assurance, mais aussi la logistique et la culture, explorent déjà les possibilités offertes par cette technologie. Les expérimentations se multiplient, les projets et les start-ups lèvent des millions d'euros sur le seul mot de blockchain. Les promesses sont à la fois techniques, économiques et institutionnelles. Dix ans après l'apparition du bitcoin, force est de reconnaître cependant que la technologie sous-jacente n'a pas encore trouvé d'usage majeur, diffusé dans le grand public. De fait, la blockchain n'a pas atteint sa maturité et les écueils sur sa route ne manquent pas, même si le nombre impressionnant de projets dans le monde entier laisse penser que les obstacles seront un jour levés.

On l'aura compris, le champ des possibles est encore très ouvert. Le rapport a le mérite de nous présenter les enjeux de cette innovation numérique en pleine mutation, sans se perdre dans la complexité technique. Plusieurs enseignements se dégagent de l'analyse.

Tout d'abord, dans la grande variété des usages envisagés, les plus porteurs de modifications profondes concernent des applications couplant sans intermédiaire la dimension transactionnelle au monde physique – ce qu'on appelle « l'internet de la valeur ». Pour l'instant, l'instabilité des monnaies numériques et la spéculation qui les

entourent empêchent la mise en place pérenne de ces applications. Mais quelques projets privés visent à trouver des solutions et plusieurs banques centrales s'en préoccupent sérieusement.

Ensuite, il apparaît de plus en plus impossible de favoriser le développement des blockchains sans se préoccuper de l'utilisation des cryptomonnaies – bitcoin, ether ou autres. Les liens techniques et économiques sont nombreux. Pour qu'innovation et sécurité coexistent, il convient dès lors de mettre en place des régulations qui soient raisonnablement attractives pour les investisseurs et les entrepreneurs mais aussi suffisamment strictes pour contrôler et éliminer les usages frauduleux, protéger l'ordre public et le consommateur-épargnant.

Encourager l'essor des blockchains et organiser l'utilisation des actifs numériques sont en fait les deux facettes d'une politique que l'on retrouve avec des pondérations variées partout dans le monde. Le jeune et dynamique écosystème français semble globalement demandeur de cette double démarche. En tout état de cause, la coordination des réglementations sur les cryptomonnaies au niveau mondial est nécessaire.

Dans le monde du numérique, les « vainqueurs » sont peu nombreux et ils ont tendance à rafler l'intégralité de la mise. Leur puissance tient à la création d'effets de réseau qui deviennent autant de barrières à l'entrée pour la concurrence. Attendre qu'une technologie soit éprouvée pour se lancer, c'est prendre le risque de partir trop tard, quand les places sont prises. Il en sera peut-être ainsi pour la blockchain. C'est donc maintenant qu'il faut « sortir du bac à sable » de l'expérimentation, et mettre en place une stratégie avec pour axes principaux la régulation, le soutien à l'innovation et la formation. Il est sans doute trop tôt pour prédire l'avenir de la blockchain et l'ampleur des bouleversements qu'elle amorce, mais l'ignorer n'est pas une option.

Cette technologie nouvelle est une expérience d'abord informatique et économique mais aussi sociale et politique. Les pouvoirs publics ont d'autant plus leur rôle à jouer que l'ensemble des acteurs semblent aujourd'hui en attente d'une intervention responsable, qui serait capable d'encourager le mouvement en tenant les deux bouts de la chaîne, entre régulation et soutien à l'innovation.

Joëlle Toledano
Présidente du groupe de travail



SOMMAIRE

SYNTHÈSE	9
INTRODUCTION	17
CHAPITRE 1 – UNE TECHNOLOGIE DISRUPTIVE ?	19
1. Bien plus qu’une chaîne de blocs	19
2. Des caractéristiques séduisantes	21
3. Chaînes publiques et chaînes privées	23
CHAPITRE 2 – QUE FAIRE DU BITCOIN ?	27
1. Naissance et fonctionnement	28
2. La grande vague des cryptomonnaies	29
3. Bulle spéculative et valorisation	33
CHAPITRE 3 – DES PROMESSES À LA CHAÎNE	38
1. Deux champs principaux	38
2. Dans tous les secteurs d’activité	43
3. Des limites surmontables ?	49
CHAPITRE 4 – LES POUVOIRS PUBLICS ENTRE SOUTIEN À L’INNOVATION ET RÉGULATION	55
1. Un intérêt mondial	55
2. L’expérimentation par les banques centrales et les réflexions en cours	57
3. Vers la régulation ?	58
CHAPITRE 5 – RECOMMANDATIONS	63
CONTRIBUTIONS DU GROUPE DE TRAVAIL	71
Des racines libertariennes à la bienveillance du monde économique, par Clément Gasull	73
Les enjeux juridiques de la blockchain. Rapport du sous-groupe juridique	85

ANNEXES

Annexe 1 – Lettre de mission.....	127
Annexe 2 – Composition du groupe de travail	129
Annexe 3 – Liste des rencontres et auditions	131
Annexe 4 – Applications des blockchains aux jeux en ligne	
Extrait d’une note interne de l’ARJEL	135



SYNTHÈSE

SORTIR LA BLOCKCHAIN DU BAC À SABLE

Pour mettre pleinement à profit une innovation, il faut penser neuf. La technologie de la blockchain nous y invite, à moins qu'elle ne nous y contraigne. En un mot, il s'agit d'une nouvelle façon de stocker de l'information, de la préserver sans modification, d'y accéder et d'intégrer de nouvelles informations qui deviennent infalsifiables. Ces nouvelles données peuvent résulter de l'exécution d'une opération, d'une transaction ou de l'exécution « automatique » d'un programme informatique. Elles sont inscrites sur l'équivalent d'un vaste registre « distribué », c'est-à-dire partagé sur les ordinateurs de tous les membres du réseau, un système qui permet transparence et auditabilité. Dans une telle architecture, les questions de contrôle et de sécurité se trouvent radicalement modifiées.

On conçoit l'ampleur des mutations que promet une telle innovation. Techniquement, elle pourrait offrir une solution aux fragilités des systèmes centralisés. Économiquement, elle devrait permettre d'augmenter la productivité en limitant les intermédiaires et en automatisant les transactions. Institutionnellement, elle est une réponse à la défiance dont souffrent les institutions politiques et économiques, avec à la clé une fluidification des relations économiques et sociales.

La blockchain est donc une technologie promise à un bel avenir. Dans la grande variété des usages envisagés, deux grandes catégories se dégagent.

- *Les applications de type « notarial » liées à la tenue d'un registre* qui a vocation à être partagé. La blockchain pourrait modifier les modalités de contrôle des transactions, de transfert de biens et d'échanges entre personnes, et au-delà la certification des processus industriels ou financiers. On attend en particulier son utilisation dans la traçabilité des médicaments ou des produits alimentaires ; elle pourrait aussi donner jour à des systèmes sécurisés de vote en ligne ou d'identification numérique des personnes.

- *Les applications couplant la dimension transactionnelle au monde physique*, ce qu'on appelle « l'internet de la valeur ». Une transaction peut être déclenchée par une intervention directe ou par l'exécution d'un programme informatique susceptible de comporter des conditions ou des vérifications particulières, par exemple sur la date ou à partir d'informations venant du monde physique. Avec de tels « *smart contracts* », les blockchains ouvrent l'ère des transactions programmables, sans intervention d'un tiers de confiance. Ces applications visent à créer de la confiance là où elle fait défaut ou à se substituer à des mécanismes de confiance centralisés. En supprimant les intermédiaires et en décentralisant les processus de validation, elles doivent permettre des gains de productivité substantiels.

À ce jour, cependant, les cas d'usage réellement opérationnels sont rares. De fait, si on veut rendre effectives les potentialités de la blockchain, il faudra surmonter de nombreuses difficultés de nature diverse.

Les enjeux sont techniques

Scalabilité. Les protocoles Blockchain, qui pour l'heure gère des données restreintes, supporteront-ils le changement d'échelle en cas de diffusion massive ? Le réseau Bitcoin par exemple traite une poignée de transactions par seconde, contre plusieurs milliers pour un opérateur de carte bancaire. Le mécanisme de validation historique de la blockchain, avec ses nœuds multiples et ses procédés cryptographiques, est source de lenteur. Les solutions techniques passent par des mécanismes de validation moins lourds, mais par conséquent moins fiables.

Protocole de consensus. Qui a accès à la blockchain, qui définit les modalités d'un ajout sur la chaîne, comment décider d'une évolution du protocole ? Le choix du « protocole de consensus distribué » est une question éminemment stratégique. La blockchain peut être publique, avec une architecture ouverte, ou privée, avec un nombre volontairement limité de participants et la réintroduction d'une forme d'autorité centralisée. L'enjeu technique se fait ici enjeu de gouvernance.

Identité électronique. Les applications requièrent que soit traitée au préalable la question de la vérification de l'identité électronique des biens ou des personnes, puisque la blockchain sert de support d'enregistrement sécurisé des transactions. Les questions des modalités – et de l'éventuelle fragilité – de l'interfaçage entre le monde numérique et le monde « réel » sont au cœur de la nouvelle technologie.

Consommation électrique. Les opérations de vérification, de validation et de cryptographie sont très consommatrices en électricité. Même si les chiffres sont contestés, une large diffusion des blockchains pourrait entraîner une externalité environnementale fortement négative. L'enjeu technique se fait ici enjeu environnemental.

Les enjeux sont monétaires et financiers

Volatilité et spéculation. Bâties sur la technologie blockchain, les cryptomonnaies se sont multipliées ces dernières années : il en existe aujourd'hui plus de 1 500, avec une capitalisation totale supérieure à 300 milliards d'euros. Mais la grande volatilité de leur cours empêche de construire des modèles économiques pérennes. La trajectoire récente du bitcoin – avec une envolée de son cours suivie d'une correction massive fin 2017 – a mis en évidence la dimension spéculative de ces crypto-actifs. Pour lutter contre ce phénomène, il faudrait imposer des réglementations comparables à celles qui sont appliquées aux marchés financiers, notamment concernant la manipulation de cours.

Dissociation entre blockchain et cryptomonnaies. On a voulu instaurer une sorte de cordon sanitaire entre les cryptomonnaies, considérées avec une certaine suspicion, et la blockchain, considérée comme très prometteuse. Utile dans un premier temps pour laisser se déployer l'innovation malgré les problèmes de fraude que posent certains usages des cryptomonnaies, cette séparation commence à poser problème. De fait, les protocoles de consensus qui sont au cœur des blockchains publiques reposent tous sur des mécanismes d'incitation économique qui requièrent l'émission d'un actif numérique. Cet actif permet d'inciter les différents acteurs à participer à la sécurisation du réseau – le protocole attribuant automatiquement un certain nombre de « jetons » aux validateurs des nouveaux blocs. Ce fonctionnement fait des actifs numériques une des pierres angulaires des blockchains publiques. Pour séparer le bon grain de l'ivraie et bénéficier des seuls effets souhaités des blockchains, il ne suffira donc pas d'essayer d'interdire ou de contrôler le bitcoin.

Vers une monnaie digitale de banque centrale ? Cette solution permettrait un couplage effectif entre monnaie et univers de la blockchain. Ce moyen de règlement émis par la banque centrale de nature crypto-monétaire donnerait le soutien matériel (existence d'un bilan) et institutionnel (légal et budgétaire) dont manquent aujourd'hui les cryptomonnaies. L'idée serait à l'étude au Royaume-Uni, au Canada, en Inde, en Suède, en Chine, à Singapour et en Russie. Le débat est bel et bien lancé. Un nouvel acronyme a même vu le jour, CBDC, pour *Central Bank Digital Currency*.

Une économie qui pourrait être transformée. La spéculation et les « arnaques » autour des cryptomonnaies ne doivent pas masquer l'essentiel. Ce qui explique le succès de ces crypto-actifs, c'est la promesse d'un ou plusieurs réseaux de transactions automatiques et de notariation. Nombreux sont ceux qui parient sur l'avenir de la blockchain comme hier ils pariaient sur Google et Facebook. Une fois passée la phase de mise au point, cette technologie est susceptible de bouleverser l'économie. Les échanges devenus par ailleurs totalement numérisés pourraient être certifiés. Les opérations entourant les échanges – appels d'offres, validations partielles par des tiers, règlements conditionnés, etc. – pourraient être gérés automatiquement et en confiance grâce aux *smart contracts*. En somme, l'économie deviendrait en partie programmable. En France, depuis quelques années, plusieurs acteurs institutionnels majeurs – Assemblée nationale, Consortium LabChain autour de la Caisse des dépôts, Banque de France, AMF, Trésor, MEDEF – ont porté des initiatives montrant leur volonté de favoriser le développement des blockchains en France. Un écosystème dynamique se développe progressivement, avec des startups, des cabinets de conseil et l'implication de grandes entreprises qui étudient le sujet et y dédient des ressources.

Les enjeux sont sécuritaires

Défaillances et piratages. Encore largement expérimentale, la blockchain a fait l'objet de nombreuses piratages ou bogues qui mettent à mal la promesse de confiance et d'infailibilité – même si le protocole numérique du Bitcoin apparaît aujourd'hui peu susceptible d'être pris en défaut. Une tension se fait jour entre l'allègement nécessaire des mécanismes de certification et la fragilisation des blockchains.

Lutte contre les activités illicites. Les cryptomonnaies se signalent aussi par leur capacité – qui varie avec le degré d'anonymat et de traçabilité des transactions – à permettre les paiements frauduleux (drogue, armes, blanchiment) ou l'évasion fiscale. Les transactions frauduleuses seraient en baisse en proportion mais en croissance en valeur absolue. Les pouvoirs publics de nombreux pays appellent au renforcement des politiques de lutte contre le blanchiment et le financement du terrorisme (politiques AML et KYC), en adoptant les modalités de mise en œuvre aux spécificités des cryptomonnaies.

Anonymat et traçabilité. Tout l'enjeu consiste à concilier – comme avec l'argent liquide – les attentes légitimes d'anonymat, pour la protection de la vie privée ou le secret des affaires, et les objectifs de traçabilité pour lutter contre la fraude. Des outils d'analyse commencent à se développer qui permettent de tracer les opérations par-delà le pseudonymat des transactions.

Les enjeux sont économiques et commerciaux

Extension à tous les secteurs d'activité. La blockchain ne doit pas être considérée comme cantonnée au monde de la finance qui l'a vue naître. Cette technologie qui fait l'impasse sur le tiers de confiance a vocation à se diffuser dans tous les secteurs économiques. Cette extension est déjà perceptible dans l'orientation des financements : alors que les ressources levées par ICO (*Initial Coin Offering*) étaient majoritairement destinées à des projets concernant l'amélioration des infrastructures et la finance, on assiste depuis 2017 à une diversification de plus en plus grande, en direction notamment des secteurs des médias, des jeux et de l'internet des objets.

Une technologie disruptive ? Dans la banque, l'assurance, mais aussi la logistique ou la santé, la technologie de la blockchain pourrait provoquer une véritable mutation dans la chaîne de valeur. Les plateformes numériques, qui sont des systèmes centralisés, ne sont pas à l'abri : championne de la désintermédiation, la blockchain a pu être décrite comme un moyen d'« ubériser Uber ». Les acteurs historiques doivent se préparer, mais l'histoire du numérique nous a appris qu'ils sont rarement les acteurs de la disruption, même quand ils en sont les inventeurs (à l'instar de Kodak). De fait, il est difficile pour une entreprise de développer des services concurrents à son cœur de métier et qui mettent en péril ses profits immédiats.

La logistique, premier candidat ? En tant que registre mémorisant sans possibilité de falsification toutes les opérations effectuées, la blockchain pourrait se révéler un outil révolutionnaire en matière de logistique. C'est tout le cycle de vie d'un produit qui peut être ainsi certifié. L'objectif est double : il s'agit non seulement de permettre la transparence des filières vis-à-vis des consommateurs, mais aussi de sécuriser ces filières contre les dysfonctionnements opérationnels ou contre diverses formes de commerce illicite. Plusieurs pilotes sont en cours de déploiement. Cette traçabilité des chaînes d'approvisionnement, du fabricant au consommateur, intéresse en premier lieu l'industrie agro-alimentaire (origine contrôlée, respect de la chaîne du froid, etc.), mais aussi l'industrie du luxe ou du médicament (lutte contre la contrefaçon).

Transparence et confidentialité. Les blockchains publiques permettent la traçabilité de l'ensemble des opérations effectuées, de manière transparente. Cette caractéristique va à l'encontre du secret des affaires. Parce que le registre est distribué, les informations qu'il contient en clair sont accessibles aux parties prenantes. C'est un avantage pour assurer la traçabilité des transactions mais un défaut rédhibitoire si des informations relevant du secret des affaires sont ainsi livrées, par exemple en finance ou en matière de santé. La confidentialité de l'information doit pouvoir être préservée pour respecter le secret commercial.

Les enjeux sont juridiques

Le droit de la preuve. Les certifications diverses (transferts de fonds, transactions, livraison de marchandises, création d'une œuvre originale, etc.) enregistrées sur la blockchain doivent avoir une portée probatoire avérée, sinon il faudra recourir aux tiers de confiance traditionnels. Aujourd'hui prédomine une insécurité juridique qui freine l'attrait de cette technologie auprès des opérateurs. Il faut donc conférer à la preuve de type « blockchain » une portée juridique reflétant la fiabilité revendiquée par la technologie. Après une phase où il était nécessaire de laisser se déployer les initiatives pour faciliter l'innovation, les inconvénients de l'insécurité juridique prennent le pas sur les avantages.

Fiscalité. L'imprécision qui pèse aujourd'hui sur le traitement fiscal des opérations apparaît également comme un frein au développement des blockchains en France. La nature juridique des actifs numériques reste imprécise, donc difficilement prise en compte par la réglementation. Une politique fiscale claire et adaptée aux cryptomonnaies (régime des opérations d'achat, de vente et d'échange) serait de nature à attirer des acteurs sérieux sur le territoire.

Droit au compte. Les émetteurs ou vendeurs professionnels de cybermonnaies ont la plus grande difficulté à ouvrir et à maintenir ouvert un compte bancaire classique auprès d'un établissement de crédit en France dans le cadre de leur activité. Ces difficultés s'étendent à l'ensemble des entreprises gérant des cybermonnaies dans le cadre de leur activité générale, soit parce qu'elles les acceptent comme moyen de paiement, soit parce que ces actifs numériques sont intégrés à leur offre de produit. La méconnaissance des cybermonnaies et autres actifs numériques conduit les établissements bancaires – qui ont eux-mêmes des obligations en matière d'identification précise de l'origine des fonds – à refuser automatiquement de gérer les comptes des entreprises ayant des cybermonnaies à leur patrimoine. Cela tient au caractère insuffisant des données que les plateformes d'échange exigent ou fournissent aujourd'hui à leurs clients. Un tel blocage est préjudiciable au développement du marché français et à l'attractivité de la place de Paris.

Un besoin de régulation

La plupart de ces nombreux enjeux fonctionnent comme des freins au développement de la nouvelle technologie. De fait, la révolution annoncée ne s'est pas encore produite, malgré les milliers de projets en cours. Il faut pourtant s'engager résolument, sans attendre l'arrivée à maturité de la blockchain. Certains des défis évoqués ci-dessus ne concernent pas les blockchains privées ; quant aux blockchains publiques,

c'est en les testant qu'on en améliorera la performance. On le sait, dans l'économie numérique, les effets de réseaux sont tels que les entreprises arc-boutées sur la préservation de leurs situations acquises risquent de se trouver marginalisées.

Déjà, les pays développés se mobilisent. Ils expriment d'abord une volonté accrue de contrôler les pratiques frauduleuses liées à l'usage des blockchains – en témoigne la mise à l'ordre du jour du G 20 du sujet, à la demande de la France. Ils affichent ensuite un intérêt marqué pour la technologie, et des stratégies nationales spécifiques se font jour ici et là. Du côté des industriels, quelques acteurs comme IBM cherchent à se positionner dans le développement de solutions. Pour l'instant les grands acteurs des plateformes numériques sont plutôt restés en retrait.

Après une période où la régulation semblait l'ennemi juré de l'innovation, l'heure semble venue de trouver un moyen de tenir la chaîne par les deux bouts : réguler de façon coordonnée sur un certain nombre de sujets permettra à la fois de contrôler les usages délictueux et de favoriser les développements souhaités.

Les recommandations formulées par le groupe de travail doivent être considérées comme de premières orientations au niveau national. En réalité, en matière de blockchains, c'est une réponse à l'échelle européenne voire mondiale qu'il conviendrait de viser. Les « protocoles de registres distribués » ou protocoles Blockchain revêtent des enjeux stratégiques sur lesquels la réflexion et l'action s'imposent. D'autant que nous sommes parvenus à un moment décisif pour cette nouvelle technologie. Après une période d'expérimentation sans contrainte, il est temps de « sortir du bac à sable », selon l'expression usuelle dans l'économie numérique. Par une sorte de convergence naturelle, la plupart des acteurs sont aujourd'hui disposés à entrer dans une nouvelle phase, celle d'une intervention des pouvoirs publics pour fixer un cadre juridique et réglementaire qui permette le plein essor de cette nouvelle technologie.

Sept grandes orientations

Le rapport propose les grands axes d'une *stratégie* visant réguler de façon coordonnée sur un certain nombre de sujets critiques de façon à contrôler les usages délictueux et à favoriser l'innovation et les développements souhaités. À ce stade du développement des usages, l'insécurité juridique sur des sujets de base comme la comptabilité, la fiscalité, la relation avec les banques et le manque d'expertise des pouvoirs publics sur le sujet devient néfaste, tant du point de vue du contrôle des usages délictueux que de l'accompagnement du développement industriel d'un secteur prometteur.

1. Promouvoir des travaux de recherche et développement, en veillant à favoriser l'interdisciplinarité.
2. Inciter au développement de formations approfondies et aider à l'appropriation du sujet.
3. Établir les régulations de base permettant de contrôler les usages frauduleux des cryptomonnaies et développer les usages des blockchains en s'appuyant sur un *groupe à compétences transversales, à l'intérieur de l'État*. Sur un certain nombre de sujets, il y a urgence à ce que l'État apporte des réponses coordonnées et équilibrées au regard des objectifs concomitants de soutien à l'innovation et de préservation de l'ordre public. Il faut disposer de l'appui technique nécessaire à la définition de solutions efficaces et rapidement apporter des réponses aux différentes questions réglementaires soulevées en matière de fiscalité, de droit au compte, de lutte anti-blanchiment et de traitement comptable.
4. Contribuer au financement des projets « d'infrastructure logicielle ». il est nécessaire de construire les infrastructures blockchains publiques de demain. Deux scénarios sont envisageables : ou bien encadrer suffisamment les blockchains existantes ; ou bien favoriser le développement de nouvelles infrastructures plus sécurisées. À ce jour, il est difficile de trancher le dilemme : le rapport recommande donc de mener de front les deux stratégies de « maîtrise » des blockchains existantes et d'accompagnement de l'émergence de nouvelles solutions.
5. Soutenir des secteurs correspondant à des domaines d'excellence ou d'intérêt stratégique en France : logistique, lutte contre la contrefaçon, traçabilité, banque et assurance et santé, en rendant possible la sortie du bac à sable.
6. Tester, expertiser, former et s'équiper au sein des pouvoirs publics ; analyser l'évolution des blockchains publiques ; diffuser l'information, développer et utiliser des applications non critiques.
7. Répondre aux défis auxquels se heurte l'internet de la valeur, ce qui suppose une monnaie numérique suffisamment stable pour servir de contrepartie de transactions.



INTRODUCTION

La blockchain désigne la technologie numérique ou plutôt l'architecture des technologies numériques qui a notamment permis le développement du bitcoin, cette monnaie digitale qui défraie la chronique depuis une dizaine d'années. Pour autant, ce rapport n'a pas pour objet central ni même pour point d'entrée les cryptomonnaies. Il n'est pas davantage un guide pour appréhender l'immense complexité des protocoles numériques mis en œuvre par cette innovation. Il faudrait un gros volume pour détailler une telle complexité, sans parvenir probablement ni à éclairer le lecteur ni à satisfaire sa curiosité. La compréhension technique nécessite des connaissances ou un investissement intellectuel qui ne nous ont pas semblé obligatoires pour décrire et comprendre les enjeux.

Autre parti pris du rapport : il contient peu de présentations concrètes de cas d'usage, ou seulement à titre d'illustration. De nombreux rapports et ouvrages fournissent des descriptions certes intéressantes des multiples usages envisageables mais il s'agit en général de maquettes, pour lesquelles toute annonce est prématurée. Parmi les nombreux tests réalisés, rares sont ceux qui se sont transformés en projets industriels ou en plan d'affaires. Le plus souvent, les articles qui invoquent ces cas d'usage ne présentent pas les difficultés rencontrées ni les progrès à réaliser avant la mise en place opérationnelle. Notre rapport s'efforce quant à lui d'exposer les obstacles de façon globale, car les appréciations au cas par cas font encore défaut.

De fait, les écueils sont encore nombreux pour la blockchain. Paradoxalement, le premier de ces écueils a d'abord été un atout. Il a consisté à séparer de manière assez artificielle la blockchain des cryptomonnaies en général et du bitcoin en particulier. Il s'agissait de mettre une technologie prometteuse à l'abri de la contamination par une monnaie digitale sentant quelque peu le soufre, car entachée d'une forte présomption de fraude, de blanchiment d'argent et de spéculation. Mais ce découplage n'est pas entièrement fondé. Utile dans un premier temps pour laisser se déployer l'innovation et les expérimentations, il commence à poser des problèmes sérieux qu'on ne peut plus éluder. Au-delà de cette question, si l'on veut rendre effectives les potentialités de la blockchain, il faudra surmonter de nombreuses difficultés qui sont d'ordre technique, économique, juridique et réglementaire.

Car la technologie des « chaînes de bloc » présente indéniablement de formidables atouts. Techniquement, cette nouvelle façon de stocker de l'information, d'y accéder et d'intégrer de nouvelles informations qui deviennent infalsifiables, pourrait être une réponse aux fragilités des systèmes centralisés : le caractère distribué des registres permet transparence et auditabilité¹. Économiquement, elle devrait permettre d'augmenter la productivité en limitant les intermédiaires et en automatisant les transactions. Institutionnellement, elle constitue une réponse à la défiance qui mine les institutions politiques et économiques. Et créer de la confiance, c'est déjà fluidifier et élargir les relations économiques sociales.

On mesure combien les « protocoles de registres distribués² » ou protocoles Blockchain revêtent des enjeux stratégiques sur lesquels il importe de s'interroger³. D'autant que nous sommes sans doute parvenus à un moment décisif pour cette nouvelle technologie. Après une période d'expérimentation sans contrainte, il est temps de « sortir du bac à sable », selon l'expression consacrée dans l'économie numérique⁴. Par une sorte de convergence naturelle, la plupart des acteurs sont aujourd'hui disposés à entrer dans une nouvelle phase, celle d'une intervention des pouvoirs publics pour fixer un cadre juridique et réglementaire qui permette le plein essor de cette nouvelle technologie.

Après avoir expliqué de manière succincte le fonctionnement des blockchains (chapitre 1) et la vogue des cryptomonnaies (chapitre 2), le rapport explore les nombreuses applications ouvertes par cette innovation, dans la finance mais aussi dans d'autres secteurs économiques (chapitre 3). Il passe en revue les interventions des pouvoirs publics dans divers pays (chapitre 4), avant de formuler un certain nombre de recommandations (chapitre 5).

Les lecteurs voulant pousser plus loin trouveront en fin de rapport deux contributions rédigées par les membres du groupe de travail. La première dresse le tableau des idéologies qui sous-tendent la blockchain et l'ont portée d'une inspiration libertarienne vers les faveurs du monde économique. Le deuxième document, plus technique, s'efforce d'aborder de manière concrète les enjeux *juridiques* soulevés par la blockchain (identité, *smart contract*, etc.). Ces deux pans – idéologique et juridique – viennent enrichir la perception des enjeux de la blockchain.

¹ Les transactions sont confidentielles mais restent accessibles à un régulateur.

² *Distributed Ledger Technology* ou DLT en anglais.

³ Voir les différents documents produits par le groupe de travail installé par France Stratégie : www.strategie.gouv.fr/chantiers/blockchain.

⁴ L'idée, mise en œuvre au Royaume-Uni en particulier pour les FinTech, consiste à réaliser des tests dans un environnement réglementaire favorable, baptisé « bac à sable » (*sandbox*).



CHAPITRE 1

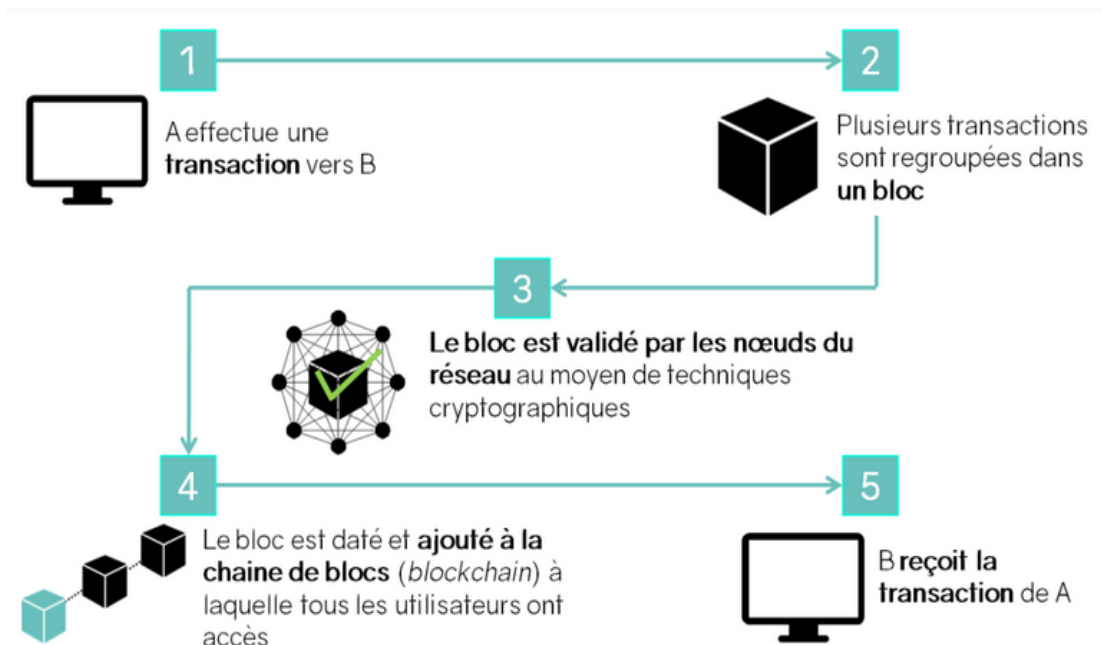
UNE TECHNOLOGIE DISRUPTIVE ?

Comment deux internautes qui ne se connaissent pas peuvent-ils effectuer une transaction – échanger de l'argent, des données, des titres financiers, des documents – de manière sécurisée et sans passer par un tiers de confiance ? Dans un monde de l'internet a priori aisément falsifiable, la technologie de la blockchain désigne l'ensemble des procédés qui réalise cette prouesse. Les paramètres techniques et les modes de gouvernance peuvent varier : qui a accès à la blockchain ? comment sont validées les transactions ? Ces questions sont les premiers enjeux de la blockchain.

1. Bien plus qu'une chaîne de blocs

Sans entrer dans la complexité technique, il suffit ici d'exposer dans ses grandes lignes le fonctionnement de ce nouvel outil. Une transaction sur internet suppose aujourd'hui la certification par un tiers de confiance – une banque, un organisme public, un notaire, un assureur, etc. Pour prévenir les tentatives de fraude, cet intermédiaire tient seul le registre des transactions. La blockchain réalise cet échange sur un réseau de pair à pair, donc sans intermédiaire. La transaction entre deux internautes est enregistrée dans un registre (*ledger*) qui garde trace de toutes les opérations effectuées. Ce registre n'est pas détenu dans un lieu centralisé mais « distribué » dans les ordinateurs de tous les participants, appelés « nœuds ». À chaque transaction, les membres du réseau interrogent l'historique pour s'assurer que la personne possède bien les actifs qu'elle souhaite échanger. Les transactions sont ensuite groupées et validées par blocs – qui forment une « chaîne de blocs » ou « blockchain ». Chaque nouveau bloc de transactions vient s'ajouter à la chaîne, lié au précédent par un procédé cryptographique. La blockchain contient ainsi l'ensemble des opérations validées depuis la création de la chaîne jusqu'à aujourd'hui. Mais c'est par abus de langage que ce premier procédé d'assemblage a donné son nom à la technologie, car il n'est qu'une composante du protocole.

Graphique 1 – Fonctionnement de la blockchain



Source : [Blockchain France 2016](#)

La véritable innovation tient davantage à la méthode de validation. La blockchain promet d'atteindre un *consensus* sur la validité des transactions. La sécurité et la décentralisation proviennent non pas du chaînage des blocs mais bien du protocole de consensus distribué. Ce mécanisme fonctionne par la « preuve de travail », en anglais « *proof of work* ». C'est ainsi que la blockchain réussit l'exploit de concilier l'ouverture au grand public et une sécurisation maximale.

Ce « *proof of work* » ou minage peut se révéler très coûteux, en temps comme en consommation électrique. D'où l'idée de recourir plutôt à la « *proof of stake* », autrement dit à la « preuve d'enjeu » (ou « preuve de possession ») : l'internaute doit prouver qu'il possède des « jetons » ou un certain montant de cryptomonnaies pour pouvoir valider un bloc supplémentaire de la chaîne. Avec la preuve de travail, on parle de mineurs ; avec la preuve d'enjeu, on parle de forgers.

Nous reviendrons un peu plus loin sur cette question centrale du protocole de consensus, qui distingue les blockchains publiques – ouvertes à tous – et les blockchains privées – avec un nombre limité de participants au réseau : ces enjeux techniques dissimulent souvent des enjeux de gouvernance.

En conclusion, pour résumer d'une phrase l'apport de la nouvelle technologie, on pourrait dire qu'internet a permis la relation et la publication directes ; et que la blockchain promet la transaction et la certification directes.

2. Des caractéristiques séduisantes

La blockchain est une sorte de gigantesque base de données qui obéit à plusieurs principes novateurs et porteurs de mutations profondes. On retient ici les caractéristiques les plus communes, en gardant à l'esprit qu'elles peuvent varier avec les usages envisagés¹.

Un système décentralisé

Contrairement à la plupart des plateformes numériques, la blockchain d'abord un système décentralisé : chaque participant possède une copie constamment mise à jour du grand registre. Il n'y a pas de serveur central mais une gestion collaborative qui est en principe une protection contre les falsifications et autres attaques. Cette désintermédiation doit aussi être un facteur de baisse des coûts.

Un système transparent

Le système est également entièrement transparent : le registre et donc l'historique des transactions est consultable en permanence par n'importe quel internaute (ou par tous les membres du réseau). Il est ainsi possible d'assurer la traçabilité intégrale d'un actif ou d'un produit ayant fait l'objet d'une transaction via une blockchain. Un participant intervient sous pseudonyme, mais toutes ses opérations sont traçables.

Un système fiable

La blockchain est infalsifiable et inviolable. Une fois enregistrées dans les blocs, les informations ne peuvent plus être modifiées ni supprimées. Avec cette technologie, le document électronique pourrait avoir autant voire plus de valeur probante que le papier. Le système décentralisé, en multipliant les copies, offre également une garantie contre le piratage.

¹ Le lecteur désireux de pousser plus loin pourra puiser dans une littérature prolifique, où se mêlent des spécialistes, académiques ou non, des passionnés de toutes origines et... des intérêts commerciaux. Pour les livres, MOOC, forums et autres blogs, on peut consulter l'abondante [bibliographie](#) francophone qui figure sur le site bitcoin.fr. Pour un manuel académique dans le sillage du célèbre MOOC de Princeton, voir Narayanan A., Bonneau J., Felten E., Miller A. et Goldfeder S. (2016), *Bitcoin and Cryptocurrency Technologies*, Princeton University Press. Voir aussi le livre de Jacques Favier et Adli Takal Bataille (2017), *Bitcoin, la monnaie acéphale*, CNRS édition. Pour une vulgarisation faite par des scientifiques, voir le blog et les articles de Jean-Paul Delahaye ou de Ricardo Pérez Marco. On lira aussi avec profit les écrits d'entrepreneurs pédagogues et de consultants comme Pierre Noizat, Vidal Chriqui ou Blockchain Partner.

Un système automatisé

La blockchain promet l'autonomie suprême, jusqu'à une forme de surveillance infaillible, sans recours à un tiers. Les transactions sont effectuées par des programmes informatiques. Des « contrats intelligents » ou *smart contracts* seront auto-exécutants.

Un système efficace

Tous les avantages de la blockchain se combinent pour promettre une efficacité économique optimale : gains de temps et coûts réduits par la suppression d'intermédiaires et l'automatisation, réduction du taux d'erreur et des contentieux, etc.

On conçoit que de tels atouts puissent retenir l'attention, à l'heure où le manque de confiance est souvent invoqué comme un des principaux freins à la croissance. Mais ces atouts ont leur revers de la médaille. Pour s'imposer, la révolution de la blockchain devra surmonter de nombreuses barrières, qui sont techniques, organisationnelles mais aussi sociétales.

Insécurité

Encore largement expérimentale, la blockchain a fait l'objet de nombreuses piratages ou bogues qui mettent à mal la promesse de confiance et d'infailibilité. Certes, le protocole numérique du Bitcoin après huit ans d'utilisation et de tentatives d'intrusion n'a jamais été lui-même pris en défaut, les attaques informatiques se concentrant sur les interfaces en tous genres et les projets plus récents. Mais plusieurs scandales visant les cryptomonnaies ont jeté le soupçon.

Criminalité

L'anonymat relatif des transactions a fait de la blockchain un refuge privilégié par les activités illicites telles le blanchiment d'argent, le trafic d'armes ou de drogue. De fait, les cryptomonnaies adossées aux blockchains sont un peu l'argent liquide du net. La lutte contre les transactions frauduleuses est un enjeu central, elle n'est pas impossible grâce à la traçabilité permise par la blockchain.

Scalabilité

Les protocoles blockchain fonctionnent car ils gèrent des masses de données encore restreintes. Trouveront-ils les solutions techniques pour supporter le changement d'échelle en cas de diffusion massive ? Pour donner une idée, le réseau Bitcoin traite une poignée de transactions par seconde quand un opérateur de carte bancaire en traite des milliers par seconde... Le mécanisme de validation historique de la

blockchain, avec ses nœuds multiples et ses procédés cryptographiques, est source de ralentissement.

Électricité

Les opérations de vérification, de validation et de cryptographie liées à la blockchain Bitcoin sont très consommatrices en électricité. Une large diffusion de cette technologie pourrait entraîner une externalité environnementale fortement négative.

Immaturité

Le mot revient souvent à propos de la technologie blockchain et de ses limites. Mais nul à ce stade ne peut dire si elle sera cantonnée et banalisée ou si elle va conquérir le monde numérique.

3. Chaînes publiques et chaînes privées

Le choix du protocole de consensus est un élément crucial des blockchains. Derrière la dimension technique de cette question se cache un fort enjeu de gouvernance.

La blockchain présente une architecture ouverte, chacun pouvant y accéder, y effectuer des transactions ou prendre part au consensus. On parle dans ce cas de *blockchain publique*. Mais cette architecture ouverte peut être modifiée en introduisant des restrictions sur les nœuds du réseau autorisés à valider les transactions ou sur l'identité des intervenants pouvant être partie à une transaction. On parle alors de blockchains *permissionnées* (« *permissioned* ») ou de blockchains *privées*, si le registre comme les transactions ne sont ouverts qu'à une liste fermée d'intervenants, par exemple au sein d'un groupe avec différentes filiales ou entre plusieurs organisations.

Cette classification en blockchain publique, blockchain permissionnée et blockchain privée est toutefois réductrice, compte tenu des nombreuses caractéristiques sur lesquelles il est possible de jouer. Les tableaux ci-dessous présentent deux exemples de classifications. En pratique, ces découpages sont toujours imparfaits : avec les logiciels open source utilisés dans les blockchains, il est possible de créer de nombreuses variantes et de jouer sur de multiples paramètres, selon les usages envisagés. Certains de ces paramètres sont d'ordre technique, d'autres relèvent de la gouvernance du dispositif.

Tableau 1 – Différents types de blockchain

Type de blockchain	Nom	Lecture du registre	Réalisation d'une transaction	Validation	Exemple
Ouverte	Blockchain publique sans permission	Ouverte à tous	N'importe qui	N'importe qui, à condition de réaliser un investissement significatif en puissance de calcul (<i>proof of work</i>) ou dans la détention de cryptomonnaie (<i>proof of stake</i>)	Bitcoin, Ethereum
	Blockchain publique permissionnée	Ouverte à tous	Participants autorisés	Tout ou partie des participants autorisés	Sovrin
Fermée	Consortium	Restreinte aux participants autorisés	Participants autorisés	Tout ou partie des participants autorisés	Banques opérant un registre partagé
	Privée permissionnée (blockchain d'entreprise)	Totalement privée ou limitée à un ensemble de nœuds autorisés	Limitée à l'opérateur du réseau	Limitée à l'opérateur du réseau	Registre interne à une banque partagé entre des filiales

Source : Global Blockchain Benchmarking study, Dr Garrick Hileman et Michel Rauchs, 2017

Nom	Contenu	Accès	Identité	Validation	Incitation
Bitcoin	Transactions monétaires	Ouvert à tous (public)	Pseudonyme	Preuve de travail	Génération de nouveaux bitcoins et ajustement de la difficulté de la preuve de travail;
Ethereum	Transactions, <i>smart contracts</i>	Ouvert à tous (public)	Pseudonyme	Preuve de travail – en transition vers un modèle de preuve de participation	rémunération en éther. Consommation de gaz en fonction de la quantité de calcul distribué pour exécuter les <i>smart contracts</i>
Ripple	Transactions financières	Restreint au monde financier. Publicité des informations de transaction mais pas des informations de paiement	Identité réelle	Vote sur la correction des transactions entre les validateurs (avec un seuil de 80 %)	Monnaie associée XRP (Ripples)

Source: adapté de Berbain C. (2017), « La Blockchain : concept, technologies, acteurs et usages », in Réalités industrielles, août.

Trois paramètres – parmi d'autres – donnent lieu à de nombreuses variantes.

- *L'identité* peut être un pseudonyme généré de façon autonome par toute personne souhaitant utiliser la chaîne, une identité réelle vérifiée par un tiers certificateur, répondant par exemple à des obligations réglementaire (KYC).
- *L'incitation à maintenir le registre* et à valider les transactions peut passer par l'attribution de cryptomonnaie pour la validation des transactions, typiquement

dans le cas d'une blockchain publique. Elle peut utiliser un autre mécanisme d'incitation, par exemple en conditionnant la possibilité de réaliser des transactions au fait de valider d'autres transactions, par exemple dans le cas d'IOTA¹. Elle peut enfin recourir à un mécanisme de gouvernance externe à la blockchain qui assure la validation des transactions (accord contractuel entre parties prenantes, typiquement dans le cas d'une blockchain privée comme SetL).

- *L'information inscrite sur le registre* peut prendre différentes modalités, depuis une publicité totale des informations de transaction (montant, destinataire), une information chiffrée limitée à l'empreinte d'une transaction, jusqu'à un chiffrement complet des données avec un accès réservé aux seules parties prenantes.

Le choix du protocole de consensus – qui définit les modalités d'un nouvel ajout sur la chaîne – est une des questions essentielles des blockchains, au cœur de nombreux débats techniques. Dans les blockchains publiques, comme Bitcoin ou Ethereum, le protocole récompense les validateurs (les mineurs du Bitcoin) en cryptomonnaie pour leur « travail de validation », ce qui les conduit à bien se comporter, c'est-à-dire à assurer l'intégrité du registre, pour préserver leurs intérêts².

Il n'existe donc pas seulement une blockchain publique et une blockchain privée mais un continuum de variantes. Les puristes y voient déjà un pervertissement fondamental du projet initial : de fait les blockchains permissionnées ou privées réintroduisent sous une forme différente une autorité centrale et un tiers de confiance en modifiant certains paramètres (taille des blocs, acteurs et durée de validation, récompense obtenue, etc.). Il n'y a plus « la » mais « des » blockchains. Ce foisonnement est une forme de banalisation : le nouveau protocole tendrait alors à devenir un simple procédé technologique, adaptable selon les contextes, et non plus une infrastructure révolutionnaire.

Conclusion

La blockchain est-elle une technologie disruptive ? Il est trop tôt pour le dire : il faudra des années avant qu'elle se diffuse dans l'économie et dans la société. Cela tient au fait qu'il s'agit d'une technologie d'infrastructure, sur laquelle viendront de manière progressive se greffer de nombreuses applications. Les variantes qui se font jour laissent penser que l'avenir pourrait éloigner la blockchain de son projet initial. La

¹ IOTA s'appuie sur une architecture de graphe acyclique et non de chaînes de blocs.

² Le chapitre 3 du rapport de l'ENISA illustre clairement le lien entre protocole de consensus, registres distribués et mineurs pour qualifier les différentes formes de blockchains. ENISA (2016), *Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector*, décembre.

récupération de cette technologie par les banques comme par les institutions publiques porte en germe un renversement spectaculaire, car cela revient à établir une gouvernance non algorithmique et à réintroduire avec des modalités différentes le tiers de confiance. La technologie de la blockchain pourrait alors se banaliser, aux deux sens du terme. Toutefois, l'histoire du numérique nous a aussi appris que les acteurs historiques d'un secteur sont rarement les acteurs de la disruption, même quant à l'instar de Kodak ils en sont les inventeurs. Il est en effet très compliqué pour une entreprise de développer des services concurrents à son cœur de métier et qui mettent en péril ses profits immédiats.

Quoi qu'il en soit, avant son éventuelle diffusion dans l'économie et la société, la technologie de la blockchain, quand elle est envisagée pour ses usages les plus innovants, est indissociable d'un produit dont elle a sous-tendu la montée en puissance : le bitcoin ou plus précisément l'ensemble de ce que l'on appelle les cryptomonnaies constituent aujourd'hui la partie émergée de la blockchain.



CHAPITRE 2

QUE FAIRE DU BITCOIN ?

Le bitcoin¹ est la première application de la Blockchain. Il en est à la fois l'origine et l'illustration emblématique, au point que protocole Bitcoin et Blockchain font parfois office de synonymes. Mais ce lien originel se révèle à double tranchant. Souvent regardée comme un objet sulfureux, la monnaie digitale pourrait entraver l'essor d'une technologie au fort potentiel disruptif. On n'en assiste pas moins depuis quelques années à la multiplication des monnaies virtuelles ou cryptomonnaies², sous l'œil hésitant des pouvoirs publics et des autorités de régulation. La trajectoire récente du bitcoin – avec une hausse spectaculaire de son cours suivie d'une correction massive fin 2017 – met en évidence la dimension spéculative de ces monnaies digitales, une bulle qui n'est pas sans rappeler la « dotcom bubble » ou « bulle internet » du début des années 2000. Reste que la blockchain est à ce jour la technologie la plus susceptible de donner corps à ce vieux rêve de l'internet, une monnaie électronique³.

¹ La cryptomonnaie est notée avec un b minuscule, par opposition au protocole Bitcoin, notée traditionnellement avec un B majuscule. D'autres blockchains rendent plus explicite la différence, notamment la Blockchain Ethereum, qui porte un nom distinct de la cryptomonnaie « ether ».

² Une cryptomonnaie « est une monnaie virtuelle utilisable sur un réseau informatique décentralisé, de pair à pair. Elle est fondée sur les principes de la cryptographie et intègre l'utilisateur dans les processus d'émission et de règlement des transactions (...) Toutes les cryptomonnaies sont des monnaies alternatives, car elles n'ont de cours légal dans aucun pays (...) De nombreuses cryptomonnaies ont été développées mais la plupart sont similaires et dérivent de la première implémentation complète : le bitcoin » (site Wikipédia, consulté le 28 mars 2018).

³ Dès 1999, l'économiste Milton Friedman y voyait la prochaine étape décisive après la création d'internet : « La seule chose qui manque, mais qui sera bientôt développée, c'est une monnaie électronique fiable (*a reliable e-cash*), une méthode permettant de transférer sur internet des fonds de A à B, sans que A connaisse B ou que B connaisse A. »

1. Naissance et fonctionnement

Le bitcoin a fait son apparition dans le sillage de la crise financière de 2008. Ce « système d'échange de liquidités de pair-à-pair » a été présenté pour la première fois dans un article d'une dizaine de pages écrit sous le pseudonyme de Satoshi Nakamoto¹. Il a vu le jour peu après, en 2009. Ce système de paiement en ligne qui fait l'économie des intermédiaires financiers grâce à une preuve cryptographique a été créé en réaction à la crise de confiance à l'égard des institutions financières. Techniquement portée par des geeks, l'idéologie sous-jacente du bitcoin est d'inspiration libertarienne et crypto-anarchiste. Elle avait donné lieu à d'autres essais non concluants depuis le début des années 1980².

Après un démarrage peu remarqué, deux mouvements contradictoires ont contribué à la notoriété du bitcoin auprès d'un public de plus en plus large. D'une part, le terme a été rapidement associé à certaines utilisations frauduleuses, entre blanchiment d'argent et commerces illicites. De l'autre, on a vu se multiplier les déclarations tonitruantes venues d'observateurs reconnus. Début 2014, Marc Andreessen, gourou et financier réputé de la Silicon Valley, comparait ainsi sur son blog l'arrivée du bitcoin à l'apparition du PC en 1975 ou à l'émergence d'internet en 1993³.

Depuis la création du bitcoin, l'ensemble des transactions exécutées dans cette monnaie digitale sont enregistrées dans un grand livre de compte, la blockchain Bitcoin. Pour valider une transaction, il suffit de vérifier dans ce registre que la

¹ Nakamoto S. (2008), « [Bitcoin : A Peer-to-Peer Electronic Cash System](#) », manuscrit. Voici l'abstract de l'article : « *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone* ».

² Voir en fin de volume la contribution de Clément Gasull consacrée aux idéologies qui sous-tendent la blockchain. On se reportera également à l'ouvrage de Jacques Favier et Adli Takkal Bataille (2017), *Bitcoin, la monnaie acéphale*, CNRS édition.

³ « *A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers (...) What technology am I talking about? Personal computers in 1975, the Internet in 1993, and – I believe – Bitcoin in 2014.* » In [Why Bitcoin Matters](#), 21 janvier 2014, NYTimes.com.

personne qui initie une transaction détient bien les fonds qu'elle souhaite transmettre. Comme on l'a vu, cette opération de validation est le fait d'acteurs particuliers, les mineurs, qui sont directement rémunérés pour cette opération. Le fonctionnement de cette monnaie digitale ne dépend d'aucune banque ou institution : il est assuré de façon décentralisée par des milliers de serveurs suivant un protocole informatique dont le code source est ouvert et utilisable par tous. Sa valeur n'est pas assise sur une contrepartie dans le monde physique. Le nombre de jetons émis à ce jour – 16,8 millions en janvier 2018 – dépasse les 80 % du total à émettre, qui doit plafonner à 21 millions, selon une loi d'émission prédéterminée qui tend vers zéro en baissant tous les 210 000 blocs. À ce rythme, on calcule que l'émission devrait s'arrêter vers 2140.

Le protocole Bitcoin mobilise des progrès réalisés pendant le dernier quart du xx^e siècle, en particulier le chiffrement asymétrique, les mécanismes de compression, la transmission d'information sur un réseau pair-à-pair, la blockchain, la preuve de travail, un mécanisme incitatif du minage¹. En résolvant le problème dit de « la double dépense », le protocole du bitcoin crée un fichier numérique répliquable et modifiable à l'infini – ce qui assure sa pérennité – mais dont toutes les copies sont dans les faits identiques, ce qui crée bien un registre numérique unique. Il résout le problème du transfert des actifs numériques sans tiers de confiance, dans un monde numérique où conserver un document (ou tout fichier numérisé) est compatible avec l'envoi à des tiers et où donc la copie est non seulement aisée mais gratuite. Avec ce protocole, une fois envoyé, malgré l'absence d'autorité centrale, le bitcoin n'appartient plus à l'émetteur. Cette performance est perçue comme une véritable prouesse intellectuelle.

2. La grande vague des cryptomonnaies

Depuis sa création il y a une dizaine d'années, le bitcoin n'a pas cessé de défrayer la chronique, à des titres divers². Intrigués par cet objet nouveau, d'innombrables articles se font l'écho des bogues, fraudes, rançons, piratages (« *hacking* »), arnaques (« *scams* ») et autres manipulations de cours, dont les modalités

¹ Voir Favier J. et Takkal Bataille A. (2017), *op. cit.*, ou Collomb A. et Sok K. (2016), « [Blockchain et autres registres distribués : quel avenir pour les marchés financiers ?](#) », in *Opinions & Débats*, Institut Louis Bachelier, n° 15, mai. Pour une vision plus académique, voir Narayanan A. et Clark J. (2017), « [Bitcoin's Academic Pedigree](#) », *Communications of the ACM*, vol. 60, n° 12, p. 36-45, décembre.

² Voir par exemple le cahier spécial des *Échos* du 19 janvier 2018. Le bitcoin a fait l'objet d'articles dans un vaste éventail de publications de la presse écrite, dans *Le Monde* mais aussi *Les Inrocks* et jusqu'à *Vanity Fair*...

surprennent les observateurs du vieux monde¹ : se disant victime d'un piratage, la plateforme d'échanges de bitcoin Mt Gox aurait ainsi vu soudain s'envoler des centaines de millions de dollars. Dans un tout autre registre, on découvre aussi avec stupeur que la consommation d'énergie nécessaire au fonctionnement du Bitcoin est de l'ordre de la 60^e plus grosse consommation nationale dans le monde² : selon les sources et les années, le bitcoin consommerait autant d'électricité qu'un pays comme le Danemark ou l'Irlande. D'autres articles insistent sur le boom des blockchains, avec un nombre d'emplois multiplié par 2 en 2017 aux États-Unis³.

L'engouement et la fascination pour une technologie un peu mystérieuse ont conduit en 2017 à un véritable emballement médiatique et financier. Un phénomène qui n'était au départ qu'une curiosité pour *geeks* a basculé dans la catégorie des sujets de première attention pour les plus grandes institutions financières (FMI), les banques (Goldman Sachs), les régulateurs (SEC, AMF, etc.) et les pouvoirs publics (Trésor, Banque de France, etc.).

En l'espace de quelques mois, sur la seule année 2017, le bitcoin a vu sa valeur multipliée par 14. Fin décembre, il dépasse même les 16 000 euros... pour retomber aux alentours de 6 000 euros début 2018 (voir Graphique 1). Ce cours valorisait les quelque 18 millions de bitcoins existants à près de 200 milliards d'euros au 31 décembre 2017.

¹ Voir par exemple *The Guardian*, « [A history of bitcoin hacks](#) », 18 mars 2014 ; ou « [Manipuler les cours du Bitcoin: est-ce bien légal ? Quels risques en cas de manipulation de cours de crypto-monnaies ?](#) » sur le blog de l'avocat Thierry Vallat (23 décembre 2017). Voir aussi la rubrique consacrée aux « arnaques » du Bitcoin [sur le site de Cointelegraph](#).

² [www.digiconomist.com](#). Ces évaluations sont contestées. [Sur son blog](#), l'analyste Marc Bevand estimait en février 2017 que les évaluations de Digiconomist devaient être divisées au moins par 2. En tout état de cause, les quantités d'énergie restent considérables et croissantes... Jean-Paul Delahaye, professeur à l'université de Lille, montre sur son blog scientifique en quoi il s'agit d'un problème structurel à résoudre – « [Ne nions pas le problème électrique du Bitcoin](#) ».

³ [www.coindesk.com](#).

Graphique 1 – Cours du bitcoin, de juillet 2017 à mai 2018, en dollars

Source : <https://bitcoin.fr/cours-du-bitcoin/>

Et le bitcoin n'est pas seul : une myriade d'autres cryptomonnaies – Ethereum, Litecoin, Ripple, Dash, etc. – aux caractéristiques plus ou moins proches, sont apparues dans son sillage¹. Un site dédié en dénombrait plus de 1 500 le 28 février 2018², avec une capitalisation de 332 milliards d'euros, dont 44 % pour le Bitcoin et 21 % pour l'Ethereum. Chacune des dix-huit premières cryptomonnaies avaient ce jour-là une valorisation supérieure à 1 milliard d'euros.

Certes, l'ensemble représente « seulement » 7,5 % de la masse monétaire de l'euro en circulation sous la forme de pièces et de monnaies et des dépôts à vue des agents non financiers (M1). Mais le montant est désormais loin d'être négligeable. Cette hausse spectaculaire de la valorisation des cryptomonnaies s'est accompagnée de fluctuations de grande ampleur, parfois de plus de 30 % en une seule journée. L'attention du grand public autour de ces fluctuations a augmenté à proportion du nombre de possesseurs de cryptomonnaies partout dans le monde : ils seraient actuellement en France plusieurs centaines de milliers³.

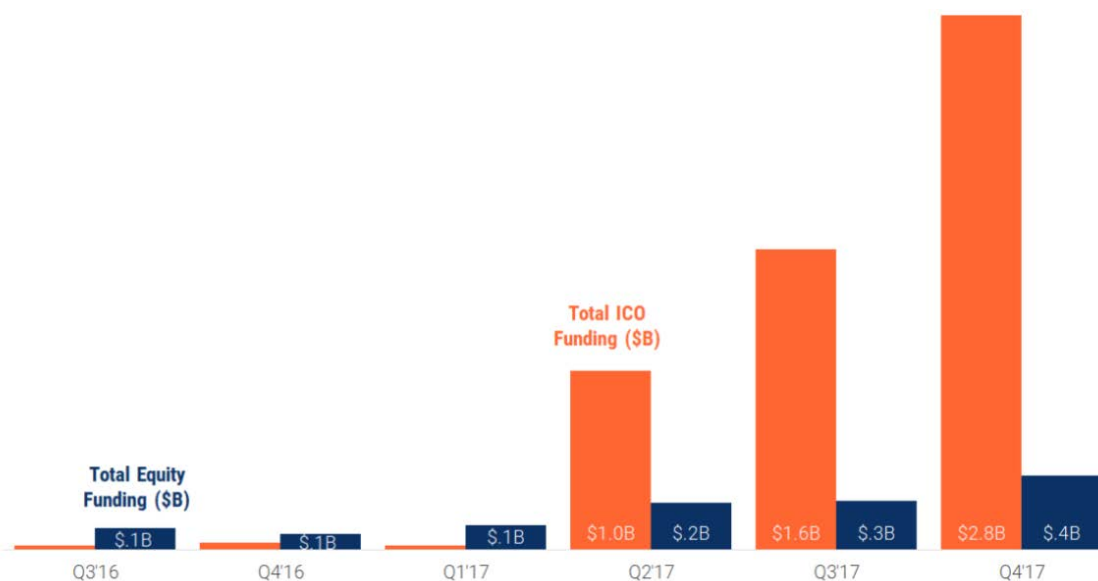
¹ Les fluctuations ont évidemment continué depuis : le 28 février, les chiffres étaient de 8 700 euros pour un bitcoin, soit une capitalisation de 146 milliards d'euros et une capitalisation de l'ensemble des cryptomonnaies de l'ordre de 330 milliards d'euros (*in* coinmarketcap.com).

² Le site [CoinMarketCap](https://coinmarketcap.com) donnait 450 milliards de dollars pour le 28 février 2018 et 328 milliards pour le 30 mai 2018. La valorisation a atteint 830 milliards de dollars lors de son pic début janvier 2018.

³ Début 2017 le rapport *Global Cryptocurrency Benchmarking Study* de Garrick Hileman et Michel Rauchs de l'université de Cambridge évaluait le nombre d'utilisateurs uniques de portefeuilles (« *wallets* ») de cryptomonnaies dans le monde entre 2,9 et 5,8 millions. L'examen de l'évolution du nombre de clients dans différents « *exchanges* » montre au moins un doublement.

Simultanément, les réalisations utilisant la technologie sous-jacente de la blockchain se sont multipliées. La Blockchain Ethereum s'est révélée redoutablement efficace pour lever des fonds au moyen d'opérations appelées *d'initial coin offering* ou ICO¹. Parfois sur la base d'un simple livre blanc décrivant succinctement le projet, des dizaines de millions d'euros ont pu être levés en cryptomonnaie (pour l'essentiel en bitcoin ou en ether) par des porteurs de projet. On parle d'un montant total entre 4 et 8 milliards de dollars selon les sources², alors que la somme des levées de fonds traditionnelles auprès du capital-risque et concernant les blockchains est de l'ordre du milliard de dollars (voir graphique 2). De fait, l'année 2017 a été particulièrement faste pour le financement de projets et les start-ups. Cependant, l'usage effectif des fonds levés par ICO n'est pas totalement avéré : dans un article publié fin 2017, Bloomberg concluait après analyse de quelque 226 ICO qu'au moment de l'enquête seules vingt entreprises utilisaient effectivement les fonds collectés. Les justifications sont nombreuses³. On notera la présomption forte de détournements qui entoure une partie – une partie seulement – de ces levées de fonds.

Graphique 2 – La montée des ICO pour le financement des projets blockchain



Source : CB Insights « *Blockchain Startups Absorbed 5X More Capital Via ICOs Than Equity Financings In 2017* », 18 janvier 2018.

¹ Ce nom est construit sur le modèle de l'introduction en bourse, IPO en anglais.

² CB insight et Elementus.io pour l'évaluation la plus élevée. En tout état de cause, la variation dans les évaluations peut non seulement s'expliquer par le champ de la collecte mais aussi par la méthode d'évaluation (les levées se faisant parfois en cryptomonnaies).

³ Kharif O. (2017), « *Only one in 10 tokens is in use following initial coin offerings* », *Bloomberg*, 23 octobre 2017.

3. Bulle spéculative et valorisation

Cet engouement pour les cryptomonnaies a été récemment dénoncé par plusieurs économistes de renom. « Le bitcoin est une pure bulle, un actif sans valeur intrinsèque – son prix tombera à zéro si la confiance disparaît », indiquait Jean Tirole, professeur d'économie à l'École d'économie de Toulouse et prix Nobel d'économie, dans une tribune publiée le 29 novembre 2017 par le *Financial Times*¹. Ces propos visaient à attirer l'attention du grand public sur les risques que représente l'acquisition des cryptomonnaies : « Les gouvernements qui accordent encore une attention favorable aux bitcoins et aux ICO seraient bien avisés de protéger leurs citoyens et leurs institutions financières contre ces développements financièrement risqués et socialement préjudiciables. » Plusieurs éléments concourent néanmoins à la valeur économique des cryptomonnaies.

Les fluctuations de cours de très grande ampleur signalées ci-dessus illustrent clairement le caractère spéculatif des cryptomonnaies. Les cours montent avec l'espérance de gain qui attire les acheteurs, ce qui fait monter le cours selon une prophétie auto-réalisatrice. Les cours montent jusqu'au moment où la confiance du grand public disparaît, ce qui provoque l'effondrement des cours et la ruine des investisseurs. Depuis le papier-monnaie de Law jusqu'à la crise des *subprimes* en passant par la bulle Internet de 2000, le mécanisme est le même et bien caractérisé par les économistes. Mais il est difficile de déceler à un moment précis si la valeur des cours traduit l'existence d'une bulle spéculative : celle-ci n'est clairement identifiée qu'après son éclatement. Dans le cas des cryptomonnaies, le risque de bulle spéculative est avéré. Pour lutter contre ce phénomène, il faudrait pouvoir évaluer l'intérêt économique des technologies blockchains, de sorte que les anticipations sur la valeur du réseau soient mieux étayées.

Un second mécanisme expliquant la valorisation des cryptomonnaies relève de l'escroquerie. Certaines cryptomonnaies sont des systèmes de Ponzi ou des projets creux surfant sur l'appât du gain des investisseurs. La démarche initiée par exemple par l'AMF, visant à obtenir une information suffisante des organisations se finançant au moyen d'une ICO – de façon obligatoire ou facultative – est une réponse apportée à ce risque.

¹ On trouve cette tribune en français sur le blog de Toulouse School of Economics : Tirole J. (2017), « [Bitcoin et crypto-monnaies : mieux vaut prévenir que guérir](#) », 4 décembre.

En outre, la très forte concentration des détenteurs de cryptomonnaies, par exemple sur le bitcoin ou sur le litecoin¹, et l'absence de régulation de marché permettent à des gros détenteurs de cryptomonnaies de manipuler les cours en pratiquant des achats ou des ventes de façon coordonnée. Ce mécanisme accentue les fluctuations des cours, dont certains profitent. Pour lutter contre ce phénomène, il faudrait qualifier d'actifs financiers certains jetons et imposer des réglementations comparables à celles qui sont appliquées aux marchés financiers, notamment concernant la manipulation de cours².

Un autre mécanisme contribue à la valeur des cryptomonnaie : leur capacité – qui varie avec le degré d'anonymat et de traçabilité des transactions – à permettre des paiements frauduleux ou de l'évasion fiscale. Il n'existe par définition aucune évaluation fine des montants de transactions frauduleuses ou interdites réalisées grâce aux cryptomonnaies. Certains observateurs évoquent des parts de 10 % à 30 % des transactions totales. Une étude australienne récente³ fait état d'une part relative de l'ordre de 25 %, certes en baisse par rapport aux 50 % antérieurs mais en croissance en valeur absolue. Autre mouvement observé, celui du glissement des transactions réalisées sur le darkweb du bitcoin vers d'autres cryptomonnaies, en particulier Monero, qui offre une confidentialité accrue par rapport à Bitcoin et Ethereum⁴. C'est la raison pour laquelle les pouvoirs publics de nombreux pays appellent au renforcement des politiques de lutte contre le blanchiment et le

¹ Au 1^{er} mars 2018, les 100 adresses les plus riches détiennent près de 19 % du total des bitcoins et 44 % des litecoins (source bitinfocharts.com) et 1 000 utilisateurs détiendraient 40 % des bitcoins. Voir Kharif O. (2017), « [The Bitcoin whales: 1,000 People who own 40 percent of the market](#) », *Bloomberg*, 8 décembre. La concentration sur Ethereum est moins documentée, celle sur Ripple est souvent mise en avant aussi.

² Le terme de « cryptoactifs » est parfois utilisé pour désigner les cryptomonnaies, notamment par la Banque de France. Cette distinction vise notamment à bien séparer les jetons numériques ou tokens de la monnaie au sens traditionnel. Nous avons retenu le terme générique de cryptomonnaie le plus fréquemment utilisé, ce qui ne préjuge pas de la qualité de monnaie du bien numérique correspondant. Le monde numérique a l'habitude de reprendre des termes classiques et de les transformer en ajoutant une extension pour désigner un objet différent (par exemple *mail* et *e-mail* en anglais).

³ Foley S., Karlsen J. R. et Putniņš T. J. (2018), « [Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?](#) », janvier.

⁴ Un acteur très impliqué dans les cryptomonnaies, Shone Anstey, directeur général de Blockchain Intelligence Group, estimait mi-2017 que la part des transactions illicites en bitcoin était passée de près de 50 % à 20 % en 2016 et continuait à baisser, alors que ces transactions se déportaient vers d'autres monnaies. Voir Cheng E. (2017), « [Dark web finds bitcoin increasingly more of a problem than a help, tries other digital currencies](#) », sur le site de CNBC, 29 août.

financement du terrorisme (politiques AML et KYC¹), en adoptant les modalités de mise en œuvre aux spécificités des cryptomonnaies. La Banque de France a formulé des propositions en ce sens².

La valeur des blockchains ne saurait se réduire à leur caractère d'actif spéculatif ou d'outils de financement. C'est aussi et peut-être avant tout un formidable outil de la numérisation de l'économie (incluant les transactions) et de traçabilité des stocks et des flux dont la valeur dépend des anticipations d'usage, quand bien même si ces usages ne sont pas encore totalement avérés aujourd'hui. Pour ne prendre qu'un exemple, celui des transferts de fonds internationaux ou transfrontaliers³, les caractéristiques des blockchains permettent d'ores et déjà d'obtenir des délais plus courts et des gains de productivités significatifs par rapport aux multiples opérations interbancaires que nécessitent des transferts de fonds traditionnels. Pour ce type de service rapide, le risque, même en cryptomonnaie, semble d'ailleurs plus acceptable. En tout état de cause, quand on songe à des acteurs comme Western Union dont la valorisation boursière est de l'ordre de 10 milliards de dollars, on comprend qu'une blockchain comme Ripple puisse intégrer dans sa valorisation sa capacité à réaliser ce genre de prestations. Les blockchains ont donc aussi comme valeur l'anticipation de leur rôle à venir. Il n'en demeure pas moins que la ou les blockchains qui sont là pour durer ne sont pas connues à ce jour : Bitcoin, Ethereum, Dash, Ripple... ou d'autres encore à venir. Selon les usages et les modèles économiques qui émergeront, les positions peuvent changer rapidement, comme l'a montré l'histoire des plateformes numériques par exemple, où Yahoo ou MySpace ont connu leur heure de gloire avant d'être remplacées par d'autres.

Conclusion

Certains usages de la blockchain ont eu besoin pour solvabiliser leurs investissements d'émettre de la monnaie virtuelle. L'univers de la cryptomonnaie s'est ainsi développé de manière spectaculaire. Cet essor ne doit pas occulter deux points : premièrement, le caractère éminemment spéculatif d'une partie de cet

¹ KYC pour « Know Your Customer » ou « politique de connaissance des clients » et AML pour « Anti-Money Laundering » ou lutte contre le blanchiment.

² Banque de France (2018), « [L'émergence du bitcoin et autres crypto-actifs : enjeux, risques et perspectives](#) », *Focus* n° 16, 5 mars.

³ « Payment adoption of Blockchain tech seems more imminent than cryptocurrency » in [Decrypting Cryptocurrencies: Technology, Applications and Challenges](#), J.P. Morgan Perspectives, Global Research, 9 février 2018.

engouement ; deuxièmement, l'usage qui pourrait devenir banal de la technologie blockchain pour les transmissions sécurisées. C'est cette promesse d'un ou plusieurs réseaux de transactions automatiques et de notarisation qui explique le succès des cryptomonnaies : après chaque éclatement de la bulle, les valorisations rebondissent. Autrement dit, la valorisation anticipée subsiste car nombreux sont ceux qui croient en la blockchain et qui « parient » sur l'avenir comme hier ils pariaient sur Google et Facebook et comme ils continuent de parier sur Amazon malgré les faibles résultats financiers.

Au fond, les cryptomonnaies ont perturbé notre appréhension de la blockchain, en masquant l'essentiel. Certes, la spéculation existe. Mais la valorisation des cryptomonnaies n'en est pas pour autant arbitraire. Car ce qui a de la valeur, c'est le fait que la blockchain permet – ou permettra – de réaliser des transactions dans le monde entier, sans intermédiaire, sans fraude et à un coût très faible. D'où l'intérêt que suscite cette nouvelle technologie bien au-delà du monde de la finance, auquel elle ne saurait être réduite : ses applications pourraient notamment changer en profondeur les secteurs du transport, de la logistique, de la culture, de l'administration ou de la santé.



CHAPITRE 3

DES PROMESSES À LA CHAÎNE

« *The trust machine* » titrait fin 2015 *The Economist*, avec le sous-titre suivant : « La promesse de la blockchain : la technologie derrière le bitcoin pourrait bouleverser l'économie »¹. Une distinction s'opérait alors entre la (ou les) blockchain(s) et le bitcoin lui-même, dont l'idéologie et certains usages rendaient la promotion un peu sulfureuse. Devenue une machine à créer de la confiance, la blockchain pouvait faire miroiter d'innombrables applications, dans tous les secteurs d'activité. À l'heure actuelle, peu de ces projets sont encore opérationnels mais leur profusion dans le monde entier laisse augurer que nombre de difficultés devraient être levées.

1. Deux champs principaux

Au vu des expérimentations et des projets en cours, on voit schématiquement émerger deux grands types d'application susceptibles de modifier radicalement l'organisation économique. Chacun a ses écueils, ses enjeux et ses pistes de solution.

Les projets « notariaux » liés à la tenue d'un registre partagé

En tant que vaste registre à la fois partagé et infalsifiable, la blockchain a vocation à bouleverser les modalités de contrôle des transactions, les transferts de biens et tout échange entre personnes, et au-delà encore la certification de processus industriels ou financiers. On pressent ainsi son utilisation prochaine dans la traçabilité des médicaments ou des produits alimentaires, ou dans des systèmes sécurisés de vote en ligne. Ces applications visent à instaurer de la confiance là où elle fait défaut ou à se substituer à des mécanismes de confiance centralisés.

¹ *The Economist* du 31 octobre 2015 : « [The trust machine. The promise of the blockchain. The technology behind bitcoin could transform how the economy works](#) ». Au début du même mois d'octobre, le ton avait été donné dans le monde des marchés financiers : voir Massa A. (2015), « [Blythe Masters Says Forget Bitcoin, Embrace the Blockchain](#) », Bloomberg, 6 octobre.

On conçoit dès lors toute l'importance, en France comme dans tous les États de droit, que revêt l'intégration des blockchains dans le « droit de la preuve ». Ce qui se trouve sur la blockchain doit pouvoir disposer d'une portée probatoire avérée, sinon l'investissement dans cette technologie sera sans intérêt, puisqu'il faudra *in fine* recourir aux tiers de confiance traditionnels. Que décidera par exemple un juge face à un élément de preuve émanant d'une blockchain ? Face à cette situation d'insécurité juridique susceptible de freiner l'attrait des opérateurs, l'enjeu consiste à s'assurer que la preuve de type blockchain se voit conférer une portée juridique reflétant la fiabilité revendiquée par la technologie.

Quand les blockchains sont privées ou « permissionnées », il suffit que les gestionnaires du réseau proposent aux utilisateurs autorisés une convention de preuve prévoyant que ces utilisateurs acceptent de considérer comme recevables en cas de litige des éléments techniques issus de la blockchain¹.

Quant aux applications développées avec une blockchain publique, elles requièrent au préalable que soit traitée la question de la vérification de l'identité électronique des biens ou des personnes, puisque la blockchain sert de support d'enregistrement sécurisé des transactions, qui sont signées par les parties prenantes².

Ce problème d'identité numérique n'est pas spécifique aux blockchains : il tient au lien entre le monde physique et le monde numérique. Mais dans un monde où les transactions sont réputées très sécurisées, le problème est d'autant plus sensible. Les questions des modalités et de l'éventuelle fragilité de l'interfaçage entre le monde numérique et le monde « réel » sont au cœur de la nouvelle technologie. C'est par le vol de clés privées stockées « à l'ancienne » par les plateformes d'échange que se sont produites l'essentiel des attaques informatiques et des vols dont ont été victimes les détenteurs de Bitcoin : il en a été ainsi pour la perte de 850 000 bitcoins stockés sur la plateforme d'échange Mt Gox en 2014 valorisés à l'époque 450 millions de

¹ Pour une analyse détaillée, voir en fin de volume la contribution « Les enjeux juridiques de la blockchain », fiche 3, « Preuve et signature numérique ».

² Le problème juridique semble plus simple pour la vérification de l'empreinte numérique de fichiers numériques ou des objets physiques qu'on arrive à identifier numériquement (par exemple par des coordonnées GPS, permettant d'établir un lien univoque entre un objet physique et son empreinte numérique) inscrite dans une blockchain (voir la fiche 3 du sous-rapport juridique en fin de volume). La reconnaissance d'une « bonne » blockchain supposerait une liste reconnue par les pouvoirs publics de blockchains suffisamment fiables. La question de cette identification reste ouverte. Elle pourrait nécessiter que suffisamment d'acteurs n'ayant pas un intérêt convergent participent à établir le consensus.

dollars¹, ou pour la perte de 500 millions de jetons sur la plateforme Coincheck, correspondant à une valeur de 400 millions de dollars en 2017², etc.

Si la blockchain utilisée est une blockchain publique, où la validation des transactions est ouverte à tous, il est nécessaire de mettre en place un mécanisme pour rémunérer les nœuds qui assurent la validation et l'enregistrement des transactions. Cette rémunération passe le plus souvent par une rémunération dans la cryptomonnaie associée à la blockchain³.

De nombreuses applications de type notarial sont aujourd'hui envisagées en utilisant une blockchain permissionnée ou privée dans le cadre de blockchains d'entreprises⁴. Cela suppose alors le recours à un tiers de confiance – celui qui gère le dispositif et son accès – ce qui limiterait le champ d'application des blockchains et en particulier, exclurait les champs d'application décrits ci-dessous.

Les projets couplant dimension transactionnelle et monde physique : « l'internet de la valeur »

Ce deuxième champ d'application a un potentiel de transformation de l'économie très puissant. La disparition progressive de l'argent liquide (déjà en cours en Suède) et la généralisation des paiements mobiles (WeChat ou Alipay en Chine, ApplePay aux États-Unis) sont des mouvements à l'œuvre dans un certain nombre de pays. Des solutions de type blockchain sont ici des candidates toutes désignées, même si d'autres technologies sont envisagées⁵.

Surtout, l'apport de la blockchain aux questions du paiement sous condition de réalisation de tel ou tel événement, ce qu'on appelle les *smart contracts*, est au cœur de ce champ d'application. Rappelons que ces « contrats intelligents » sont des programmes informatiques exécutés de façon autonome par un réseau reposant sur les technologies blockchain. De nombreux protocoles en ont fait leur spécialité, au

¹ *Les Échos* (2017), « [Mtgox : le mystère des 650.000 bitcoins évaporés](#) », 19 juillet.

² Nakamura Y., Tan A. et Hagiwara Y. (2018), « [Coincheck Says It Lost Crypto Coins Valued at About \\$400 Million](#) », *Bloomberg*, 26 janvier.

³ D'autres systèmes de registre distribués, comme IOTA, ne rémunèrent pas directement l'enregistrement des transactions.

⁴ Avec toute la prudence nécessaire pour interpréter ce genre de prévision, Tractica évalue le marché mondial des blockchains d'entreprise à 20 milliards de dollars en 2025 contre 2,5 milliards de dollars en 2016. Le marché européen en 2025 représenterait 5 milliards de dollars (voir [State of Blockchain 2018](#), Coindesk).

⁵ Annales des Mines (2017), « [Vers la fin du cash ?](#) », *Réalités Industrielles*, novembre 2017.

premier rang desquels Ethereum. L'internet des objets est par exemple très concerné, lui qui doit opérer sur les principes de l'autonomisation et de l'infailibilité.

Mais ces développements se heurtent au problème de la grande volatilité des cryptomonnaies. Bâtir un modèle économique de long terme, dans un monde où l'essentiel des dépenses – salaires et achats – se fait en monnaie traditionnelle, alors que les recettes se feraient en cryptomonnaies, est d'autant moins possible que l'absence d'une relative stabilité monétaire rend les utilisateurs potentiels très circonspects. On l'a vu, les cryptomonnaies restent aujourd'hui des actifs spéculatifs, dépourvus des attributs souhaités pour une monnaie (moyen de paiement, unité de compte, réserve de valeur)¹.

Dans l'absolu, deux réponses sont envisageables pour répondre à cette difficulté majeure. Soit des émissions de crypto-actifs affichant une parité fixe avec une monnaie légale ou garantissant une certaine stabilité grâce à des algorithmes. Force est de constater que de telles cryptomonnaies n'ont pour l'instant pas rencontré un grand succès et que des soupçons de fraude pèsent encore sur Tether, une des plus connues². Pour autant, de nouveaux projets soutenus par des entreprises de capital-risque réputées voient actuellement le jour³.

Une autre réponse, sur laquelle nous reviendrons dans le chapitre suivant, serait une monnaie numérique de banque centrale. Elle permettrait un couplage effectif entre monnaie et univers de la blockchain. Ce moyen de règlement émis par la banque centrale de nature crypto-monétaire donnerait le soutien matériel (existence d'un bilan) et institutionnel (légal et budgétaire) dont manquent aujourd'hui les cryptomonnaies.

Le retour au galop du bitcoin ?

Les lignes qui précèdent en témoignent : séparer les blockchains et les cryptomonnaies n'est pas aussi simple qu'on a pu le croire. De fait, les protocoles de

¹ En tout cas dans la plupart des pays, qui bénéficient d'une monnaie relativement stable et reconnue au plan international. Pour une perspective sur les termes du débat sur le statut théorique des cryptomonnaies par rapport à la monnaie, voir Faure P.-H. (2016), « Le bitcoin peut-il être assimilé à une monnaie ? Un examen à partir des différentes grilles de lecture de la science économique », document de travail, Larefi – université de Bordeaux, juin ; Lakomski-Laguerre O. et Desmedt L. (2015), « [L'alternative monétaire Bitcoin : une perspective institutionnaliste](#) », *Revue de la régulation*, vol. 18, deuxième semestre.

² *Les Échos* (2018), « [Tether, le scandale qui menace le bitcoin](#) », 6 février..

³ Voir par exemple Prezelj D. (2018), « [The quest for the stable token continues](#) », sur le site ioNectar, 6 mars. Basecoin annonce travailler sur un projet en ce sens, soutenu par Andreessen, Horowitz et Bain Capital Ventures Capital.

consensus, qui sont aujourd'hui au cœur des blockchains publiques, reposent tous sur des mécanismes d'incitation économique qui requièrent l'émission d'un actif numérique. Cet actif numérique permet d'inciter les différents acteurs à participer à la sécurisation du réseau – le protocole attribuant automatiquement un certain nombre d'actifs aux validateurs des nouveaux blocs. Ce fonctionnement fait des actifs numériques l'une des pierres angulaires des blockchains publiques.

Pour les blockchains purement privées où seules des personnes autorisées peuvent accéder à la blockchain, la création d'un actif numérique ne peut avoir qu'une fonction purement utilitaire. Par exemple, on peut imaginer des jetons, *tokens* en anglais et parfois aussi en français, qui représentent des titres financiers sur une blockchain privée gérant un marché de titres. Mais on peut imaginer bien d'autres usages, tels que les jeux en ligne, les points des programmes de fidélisation, la participation à des ICO, etc. Il n'y a d'ailleurs aucun marché hors de cette blockchain qui donnerait une valeur particulière à ces jetons numériques.

Pour les blockchains semi-privées – pour lesquelles la validation des transactions est centralisée autour d'une liste définie d'acteurs mais ouverte pour ce qui concerne les participants aux transactions – à l'instar de Ripple, l'actif numérique Ripple (XRP)¹ n'est a priori plus nécessaire à la sécurisation du réseau, qui est assurée par des acteurs centralisés. Le Ripple est vendu comme un outil de lutte contre le spam de transaction : il faut payer un peu de Ripple pour chaque transaction, ce qui permet d'éviter l'envoi massif de transactions qui ferait ralentir le réseau. Le Ripple est également utilisé comme unité de compte intermédiaire pour échanger de la valeur sur le réseau Ripple. Sa valeur de marché – près de 29 milliards d'euros au 28 février 2018 – peut être attribuée non seulement à son utilité en tant que médium de transfert de valeur mais aussi à la spéculation autour de cette valeur et de la réputation de « blockchain des banques » de Ripple.

La possibilité de lever des fonds *via* une ICO, que l'AMF envisage d'encadrer², est l'exemple le plus symptomatique de cet enchevêtrement entre le monde des cryptomonnaies et le monde réel.

¹ Le réseau Ripple s'appuie sur une cryptomonnaie particulière (acronyme XRP) construite pour le développement des usages par les entreprises et appréciée par un certain nombre de banques. Lancé en 2012, il vise à permettre des « transactions financières mondiales sécurisées, instantanées et presque gratuites, de toute taille, sans rejet de débit ». Il prend en charge n'importe quelle monnaie fiduciaire, cryptomonnaie, commodité ou toute autre unité de valeur tels que miles aériens, minutes mobile (wikipedia).

² L'AMF a lancé fin octobre 2017 une consultation publique. Elle notait dans l'exposé des motifs : « Dans le cadre des actions et du suivi qu'elle mène en matière d'innovation, l'AMF a réalisé une

Même quand on utilise des blockchains beaucoup plus contrôlées que Bitcoin et appréciées du système bancaire, comme Ripple, on a pu observer début 2018 d'énormes variations du cours de la cryptomonnaie sous-jacente, sans explication évidente. Autrement dit, pour séparer le bon grain de l'ivraie et bénéficier des seuls effets souhaités des blockchains, il ne suffira pas d'essayer d'interdire ou de contrôler le bitcoin.

2. Dans tous les secteurs d'activité

La distinction formelle opérée entre bitcoin et blockchain a eu le mérite de stimuler de nombreuses initiatives partout dans le monde. Le vaste champ d'applications et d'usages ouvert par cette technologie porteuse ne demandait qu'à être exploré. On a ainsi assisté ces dernières années au développement de nombreux démonstrateurs et tests (*Proof of Concept* ou POC), qui pourtant ont rarement débouché sur des usages commerciaux, à de rares exceptions comme les jeux en ligne (voir annexe 4).

Ce constat a été largement repris au cours des auditions menées par France Stratégie¹. Deux études réalisées en 2017 – l'une par des chercheurs de l'université de Cambridge financée par des acteurs essentiellement financiers², l'autre par le cabinet Deloitte – font le même diagnostic au niveau mondial : ils mettent en évidence le faible taux de survie des projets blockchains³.

Le déploiement opérationnel pour certains usages est cependant envisagé dans un cadre contrôlé, avec des restrictions sur les validateurs des transactions ou sur les personnes habilitées à initier des transactions, en particulier dans le secteur financier. C'est notamment le cas de ceux développés par la Banque de France, avec son application Madré⁴, et pour l'échange des minibons, titres de créance dont la détention et le transfert peuvent être enregistrés sur une blockchain, en application

première étude approfondie de ces opérations et de leurs implications juridiques. Il ressort de ce premier état des lieux que si une partie des ICO observées pourrait relever de dispositions légales existantes (...), la plupart de ces émissions resterait, en l'état actuel du droit, en dehors de toute réglementation dont l'AMF assure le respect. » La [synthèse des résultats](#) a été publiée le 22 février 2018. L'AMF y annonçait : « Le Collège de l'AMF a décidé de poursuivre le travail relatif à la définition d'un cadre juridique spécifique aux ICO » (voir le site www.amf-france.org).

¹ La liste des rencontres et auditions figure en annexe 3.

² Hileman G. et Rauchs M. (2017), [Global Blockchain Benchmarking Study](#), Cambridge Centre for Alternative Finance.

³ Deloitte Center for Financial Services (2017), [Evolution of blockchain technology: Insights from the Github platform](#), a research report, octobre.

⁴ Registre partagé entre la Banque de France et des banques commerciales partenaires, enregistré sur une blockchain et permettant l'attribution des Identifiants Créanciers SEPA.

de l'ordonnance ayant introduit dans le droit les « dispositifs d'enregistrement électronique partagé »¹. Les conditions de sécurité de ces échanges doivent cependant être encore précisées par un décret en Conseil d'État².

Un écosystème s'est aussi constitué autour des plateformes d'échange, des acteurs de « *wallets* »/portefeuilles, des mineurs, de consultants et de startups. L'écosystème, en particulier les acteurs financiers, s'est regroupé autour de ce qu'on appelle parfois les blockchains d'entreprise. Elles regroupent, le plus souvent sous la forme de consortia, toute une série d'initiatives qui visent essentiellement à contribuer au développement et à la mise à disposition d'outils en vue de développer des applications dans les entreprises³. Pour autant, aucun des nouveaux services annoncés ou envisagés n'a mis en place à ce jour un modèle économique éprouvé. Intéressé au premier chef, le secteur financier – comme celui de l'assurance – se heurte à un certain nombre de dilemmes encore rédhibitoires pour ses régulateurs français (voir l'encadré ci-dessous).

Les dilemmes de la blockchain pour le secteur financier

Extrait de « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de contrôle prudentiel et de résolution (ACPR) » par Nathalie Beaudemoulin, Didier Warzée et Thierry Bedoin, publié en août 2017 dans *Réalités industrielles*

« La nature même de la blockchain utilisée et de ses caractéristiques fondatrices (le fait d'être à la fois publique et décentralisée) continue de poser des difficultés importantes (voire rédhibitoires) pour une application à grande échelle au domaine financier. Ces difficultés peuvent être appréhendées sous la forme de quatre dilemmes :

Premier dilemme : décentralisation versus responsabilité. La décentralisation du système de confiance (qui présente des avantages notamment en termes de sécurité du dispositif partagé par un plus grand nombre) ne permet pas d'identifier un acteur juridiquement responsable de sa sécurité, qui rendrait compte aux clients (par exemple en cas de défaillance, pour assurer la continuité du dispositif, le remboursement, etc.) et aux autorités de régulation.

¹ Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.

² Voir par exemple le livre blanc de Paris Europlace, octobre 2017.

³ Pour lister les noms les plus significatifs de *consortia* : Enterprise Ethereum Alliance (avec plus de 250 membres), Hyperledger (avec plus de 100 membres), R3 (plus de 100 membres), ainsi que des initiatives d'entreprises comme IBM ou Microsoft. Voir le point réalisé par Coindesk ([State of blockchain 2018](#)).

Deuxième dilemme : liberté versus dépendance. La blockchain publique s'affiche comme un bien collectif autogéré auquel tout un chacun peut (en principe) contribuer. Or, dans la pratique, elle s'avère très dépendante de quelques codeurs. Elle est aussi très dépendante vis-à-vis de fermes de minage extrêmement concentrées sur le plan géographique et économiquement incitées à se regrouper (jusqu'à un certain point¹) (...)

Troisième dilemme : transparence versus confidentialité. La blockchain publique est transparente et efficace en termes de traçabilité des opérations. En effet, elle permet de connaître l'ensemble des transactions ou des enregistrements réalisés, à la manière d'une piste d'audit présentée comme unique et intangible. Néanmoins, cette caractéristique se heurte assez rapidement au principe du secret des affaires, chaque établissement participant ne souhaitant pas exposer (notamment à la concurrence) les transactions qu'il réaliserait en l'utilisant.

Quatrième dilemme : anonymat versus identification. Le principe libertaire qui sous-tend la blockchain implique l'usage de pseudonymes, ce qui ne permet pas l'identification des acteurs. Cette opacité n'est pas acceptable au regard des objectifs de la lutte contre le blanchiment des capitaux et le financement du terrorisme.

En raison de ces limitations, l'usage des blockchains publiques pour des activités régulées n'apparaît pas approprié à ce stade – sauf à concevoir une blockchain publique nativement construite pour répondre aux problématiques du secteur financier, incluant les enjeux de supervision.

Le découplage opéré entre bitcoin et blockchain a notamment eu pour conséquence d'accélérer la prise de conscience que les blockchains pouvaient être utilisées pour bien d'autres activités que le simple échange de valeur entre comptes. Avec les *smart contracts*, une transaction peut en effet être déclenchée par l'exécution automatique d'un programme informatique, susceptible de comporter des conditions ou des vérifications particulières, par exemple sur la date, des transactions couplées, voire des informations venant du monde physique. Les blockchains ouvrent ainsi l'ère des transactions programmables, sans intervention d'un tiers de confiance. C'est en particulier le programme précurseur des concepteurs et des promoteurs du protocole

¹ Il faut qu'elles restent en deçà de 50 % de la capacité de traitement en termes de puissance de calcul mise en œuvre, sinon elles mettent en danger l'efficacité du protocole de « preuve de travail », et donc la confiance dans le bitcoin – confiance dont elles tirent leur richesse (étant donné qu'elles sont rémunérées... en bitcoins).

Ethereum, dont la cryptomonnaie, l'ether, est la deuxième cryptomonnaie en termes de valorisation à fin février 2018¹.

Les technologies Blockchains sont ainsi perçues comme la réponse à des enjeux multiples – techniques, politiques, économiques et financiers – dans un contexte où pourtant les usages frauduleux n'ont pas disparu et où les incertitudes juridiques et fiscales persistent². Les blockchains devraient permettre **le passage de l'internet de la communication à l'internet de la valeur** en « réglant » les problèmes posés par l'absence de confiance et d'une autorité tiers de confiance pour les transactions par Internet. En baissant les coûts de mise en relation et de transaction, l'Internet 2.0 et ses plateformes centralisées ont déjà conduit à restructurer les chaînes de valeur de nombreux secteurs d'activités, de la publicité aux médias (Google, Facebook) en passant par le voyage (Booking, AirBnb) et le transport (Uber, Blablacar). Ce serait aujourd'hui au tour du secteur financier et de l'assurance d'être en première ligne face à cette nouvelle révolution numérique qui diminuerait drastiquement les coûts de transaction et de contrôle³ et permettrait de réaliser les gains de productivité que le secteur n'a pas réalisés ces dernières années, comme le montrent les travaux de Thomas Philippon⁴.

Au-delà de ces objectifs de productivité, les blockchains sont susceptibles de répondre **au problème de la méfiance** dans nos sociétés, non seulement très coûteux en économie de marché, mais dangereux politiquement et socialement⁵. Les consommateurs et citoyens sont en permanence confrontés à des problèmes de contrefaçon, d'insécurité alimentaire, d'obsolescence programmée ou de services

¹ Le nombre de transactions par jour sur Ethereum a dépassé celui réalisé sur Bitcoin depuis le milieu de l'année 2017. Source : State of Blockchain 2018, coindesk.

² Beaudemoulin N., Warzée D. et Bedoin B. (2017), « [Les enjeux de la Blockchain pour la Banque de France et l'Autorité de contrôle prudentiel et de résolution \(ACPR\)](#) », *Annales des Mines-Réalités Industrielles*, août.

³ Ito J., Narula N. et Ali R. (2017) « [The Blockchain will do to the financial system what the Internet did to media](#) », *Harvard Business Review*, 8 mars; Iansiti M. et Lakhani K. R. (2017), « The truth about Blockchain », *Harvard Business Review*, janvier-février.

⁴ Philippon T. (2015), « [Has the US Finance Industry Become Less Efficient? On the Theory and Measurement of Financial Intermediation](#) », *American Economic Review*, vol. 105(4), p. 1408-1438 ; et Philippon T. (2016), « The FinTech Opportunity », CEPR, juillet.

⁵ Sur la question de la confiance dans les relations économiques, voir pour la France Algan Y. et Cahuc P., (2016), *La société de défiance. Comment le modèle social français s'autodétruit*, CEPREMAP, Éditions de la rue d'Ulm, première édition 2007 ; et Algan Y., Cahuc P. et Zylberberg A. (2012), *La Fabrique de la défiance... et comment s'en sortir*, Paris, Albin Michel. Des analyses plus récentes concernent les États-Unis : « *Mistrust in America could sink the economy* », *The Economist*, 10 août 2017.

clients inaccessibles, de médicaments contrefaits, de pratiques financières délictueuses.

Dans le secteur de l'assurance, connu pour souffrir d'une confiance limitée de la part des consommateurs¹, Axa a récemment lancé une offre baptisée « fizzy » qui s'appuie sur le protocole Ethereum spécialisé dans les *smart contracts*. L'idée est de proposer des contrats garantissant à l'assuré une couverture maximale en cas de manquements à la ponctualité aérienne. Lorsque son avion se pose, le *smart contract* vérifie immédiatement l'heure d'arrivée, le retard éventuel, les conditions de remboursement préétablies et déclenche automatiquement si besoin la procédure d'indemnisation. Le tout sans autre formulaire ou démarche, dans le respect de l'anonymat, sans intervention même de l'assureur. C'est l'automatisme qui est une réponse au manque de confiance.

Dans le secteur de la logistique, une startup française, Tilkal, offre une plate-forme reposant sur des blockchains permissionnées, centrées sur la « notarisation » et spécialisées dans la traçabilité des chaînes d'approvisionnement, du fabricant au consommateur, avec un focus fort sur l'industrie agro-alimentaire. L'actualité a montré que ce secteur est régulièrement entaché de scandales qui minent la confiance des consommateurs, affectent négativement l'image du secteur à l'export et entraînent des risques pour la sécurité sanitaire. L'objectif ici est double : il s'agit non seulement de permettre la transparence des filières vis-à-vis des consommateurs, mais aussi de sécuriser ces filières contre les dysfonctionnements opérationnels ou contre diverses formes de commerce illicite. Plusieurs pilotes sont en cours de déploiement, y compris sur des problématiques export. C'est tout le cycle de vie d'un produit qui est ainsi certifié. Tel produit de luxe provient bien de l'atelier de fabrication de la marque et a bien emprunté le circuit homologué, tel médicament contient bien la molécule active et a transité par des revendeurs habilités, tel produit alimentaire a respecté les conditions d'élevage, sans rupture de la chaîne de froid, etc. Ce suivi intégral permet de détecter la moindre anomalie suspecte et de restaurer *in fine* la confiance du consommateur.

D'autres domaines d'applications ont été mis en évidence, qu'il s'agisse d'usages publics ou privés. Parmi les applications les plus en vue, outre la logistique, on citera l'internet des objets, la gestion des droits, la santé, l'administration (registres divers avec l'exemple fameux du cadastre, identité, votes, etc.).

¹ Voir par exemple « [80 % des Français ne font pas confiance aux assureurs](#) », sur le blog de Philippe Moati.

Les usages tels que le financement participatif (*crowdfunding*), dont l'ICO est une modalité spécifique, les transferts de fonds ou les jeux en ligne sont eux d'ores et déjà pleinement opérationnels, même si l'augmentation des coûts de transaction liée à l'augmentation des valorisations des cryptomonnaies – et en particulier du bitcoin – sont susceptibles de modifier les modèles économiques sous-jacents.

Plus généralement, les blockchains peuvent servir de support à des applications décentralisées. Les services envisagés vont des plateformes d'échange décentralisées (AirSwap, EtherDelta, Radar Relay), plateformes permettant la rémunération automatique pour la réalisation de services (GitCoin), plateformes de traçabilité (Provenance), marchés prédictifs (Gnosis, Augur), gouvernance d'entreprise sur blockchain (Aragon, GovernX), marchés de puissance de calcul sur blockchain (le français iEx.ec), produits dérivés sur blockchain (VariabL, dydx) ou même les fameux « cryptokitties¹ ».

À titre illustratif, EtherDelta est une plateforme sur laquelle les utilisateurs peuvent échanger sans intermédiaire différents tokens sur la blockchain Ethereum. Elle fonctionne comme une plateforme classique (ordres d'achat, de vente, etc.) mais l'ensemble des échanges est réglé par des *smart contracts* qui permettent aux ordres de se rencontrer et qui réalisent automatiquement les échanges lorsqu'un vendeur rencontre un acheteur. Il n'existe donc pas de plateforme centralisée détenant les fonds des utilisateurs, qui conservent la propriété de leurs actifs jusqu'au moment où l'échange est réalisé.

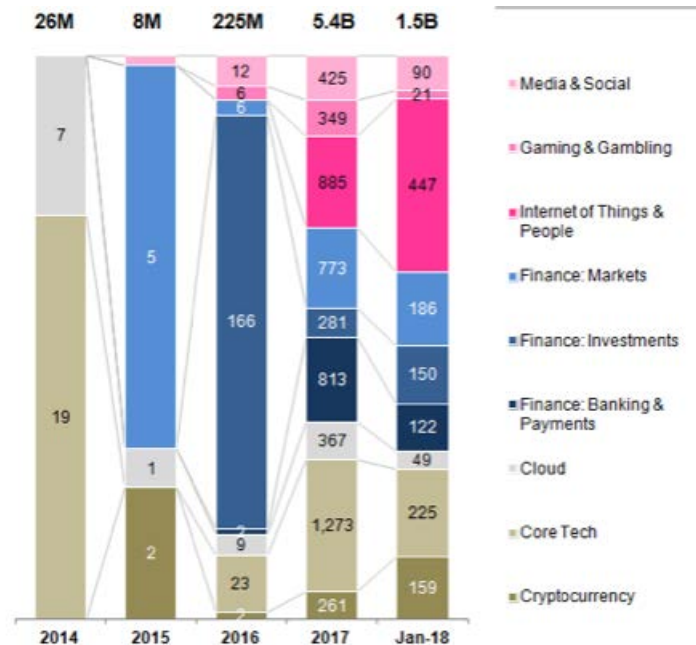
Les blockchains permettent le partage des informations sans pour autant sacrifier le besoin de confidentialité des entreprises. Dans tous les secteurs, cette technologie est susceptible d'apporter une réponse aux fragilités structurelles des systèmes centralisés, grâce au caractère distribué des registres, qui permet transparence et auditabilité. Les questions de contrôle et de sécurité sont radicalement modifiées.

Pour conclure, relevons que l'extension de la blockchain à tous les secteurs est perceptible dans l'orientation des financements. Jusqu'à 2017, les ressources levées par ICO étaient majoritairement destinées à des projets concernant l'amélioration des infrastructures et la finance. Il semble qu'on assiste à une évolution de ce côté, avec

¹ Ce jeu a connu récemment un tel succès qu'il a ralenti le service de la blockchain Ethereum en provoquant un afflux de transaction (25 % du trafic). Il aurait généré 19 millions de dollars de chiffre d'affaires en un peu plus de trois mois. Plus généralement, c'est toute l'industrie des jeux en ligne qui est concernée et qui pourrait être transformée : voir Wolfson R. (2018), « [Tokenizing Virtual Assets Using Blockchain Tech Will Disrupt the Billion-Dollar Gaming Industry](#) », Themerkle.com, 6 mars.

une diversification de plus en plus grande, en direction notamment des secteurs des médias, des jeux et de l'internet des objets (voir Graphique 3 ci-dessous).

Graphique 3 – Les fonds levés par ICO : une diversification des secteurs



Source : Autonomous Next #Token Mania, juin 2018

3. Des limites à surmonter ?

Aussi riches soient-elles, les promesses de la blockchain continuent de se heurter à un certain nombre de failles de sécurité¹, dont on trouve la trace dans les multiples piratages et arnaques observés. C'est là un écueil paradoxal pour une technologie dont une des qualités premières revendiquées est la fiabilité et l'invulnérabilité. En réalité, la sécurité du protocole Bitcoin lui-même n'a pas été mise en défaut à ce jour. Les attaques informatiques se reportent en revanche sur les interfaces de toutes sortes avec les autres systèmes – typiquement les places de marché, sujettes aux fragilités traditionnelles des systèmes centralisés.

¹ Flori J. P. (2017), « Sécurité et insécurité des *blockchains* et des *smart contracts* », *Annales des Mines-Réalités Industrielles*, 2017/3, août.

Plus généralement, les limitations des blockchains en matière de vitesse, de débit, de confidentialité, de passage à l'échelle (ou « scalabilité »), d'interopérabilité, etc., sont avérées et largement documentées¹.

Les questions de minage, au cœur de la preuve de travail sur laquelle se fonde le consensus pour le Bitcoin, font également l'objet de nombreux débats. Au plan théorique, il s'agit de définir rigoureusement les conditions permettant de se prémunir contre la malveillance des nœuds validateurs. Le niveau de 51 % de la puissance de calcul détenue par une entité malveillante est certes considéré comme le niveau de référence. Pourtant, cette valeur fait l'objet de controverses dans la communauté de la recherche². Le nombre et la répartition des nœuds sont également des sujets sensibles. Les questions économiques commencent elles aussi à mobiliser les chercheurs. Outre bien sûr les pans monétaires et financiers (concurrence entre monnaies, systèmes monétaires), les thématiques concernent l'économie du minage, avec la question des incitations coopératives à destination des mineurs³ ou l'évolution de la capacité de minage⁴. Et les débats ne s'arrêtent évidemment pas au Bitcoin puisque beaucoup dépend justement du modèle de consensus retenu pour se substituer au système de décision centralisée. En tout état de cause, des évolutions substantielles sont à venir dans l'environnement technique des registres distribués.

« Immaturité » est le terme qui revient le plus souvent à propos de la blockchain⁵. Sur son site, Ethereum France par exemple reconnaît les difficultés rencontrées : « La technologie blockchain est toujours une technologie balbutiante. Aujourd'hui, elle fonctionne, mais elle fonctionne *mal*. De façon générale, la blockchain est lente, inefficace, ne peut pas gérer beaucoup de transactions par secondes, est limitée

¹ Pour une vision d'ensemble, voir Favier J. et Takkal A. (2017), *op. cit.*, p. 202 et suivantes ; Systematic, Paris Region Digital Ecosystem (2017), « White Paper – Blockchain: myth or reality ? », chapitre 5. Voir également Primavera de Filippi qui met l'accent dans ses travaux sur les questions de gouvernance et de responsabilité, et du cabinet Gartner (2017), qui souligne les inquiétudes qui demeurent en matière de sécurité, de légalité, de scalabilité et d'interopérabilité.

² Anceaume E., Ludinard R. et Sericola B. (2016), « [Relying on consensus does not make bitcoin safer](#) », International Conference on Dependable Systems and Networks, Toulouse, juin.

³ Biais B., Bisière C., Bouvard M. et Casamatta C. (2018), « [The Blockchain Folk Theorem](#) », Toulouse School of Economics, Working Papers n° 17-817, 5 janvier (ou [Swiss Finance Institute Research Paper n° 17-75](#)). l'évolution de la puissance de minage et les capacités associés (Prat, Julien; Walter, Benjamin (2018) : An Equilibrium Model of the Market for Bitcoin Mining, CESifo Working Paper, No. 6865).

⁴ Prat J. et Benjamin W. (2018), « [An equilibrium model of the market for bitcoin mining](#) », CESifo Working Paper, n° 6865, janvier.

⁵ Voir par exemple les propos de figures emblématiques de la « communauté » comme Nick Szabo ou Vitalik Buterin.

dans ses usages. Bitcoin peut traiter au maximum sept transactions par seconde, Ethereum quinze. Le principe de faire réexaminer et réexécuter toutes les opérations par tous les participants au réseau est certes un gage de sécurité mais il ralentit fortement le traitement des opérations qui ne s'effectuent qu'en séquentiel et jamais en parallèle. Vlad Zamfir, un des développeurs principaux du protocole Ethereum, résumait récemment l'état actuel de la blockchain dans un tweet : *“Ethereum isn't safe or scalable. It is an immature experimental tech. Don't rely on it for mission critical apps unless absolutely necessary”*. (Vlad Zamfir @VladZamfir, 4 mars 2017). Ce tweet, qui a provoqué de nombreuses réactions, met finalement en avant le caractère hautement expérimental de la technologie et la nécessité aujourd'hui de fonctionner par itérations, tests... ».

D'autres limites des blockchains sont régulièrement invoquées, notamment la tension entre transparence et confidentialité, entre anonymat et identification des parties prenantes (voir encadré supra sur les « dilemmes de la blockchain pour le secteur financier »). Parce que le registre est distribué, les informations qu'il contient en clair sont accessibles aux parties prenantes. C'est un avantage pour assurer la traçabilité des transactions mais un défaut rédhibitoire si des informations relevant du secret des affaires sont ainsi livrées, par exemple en finance ou en matière de santé. Pour toute activité qui suppose de partager certaines informations en en protégeant d'autres, la possibilité de masquer l'information de façon fiable est recherchée par le marché.

De même, l'identité des intervenants n'est pas connue quand les parties d'une transaction utilisent des pseudonymes. Des possibilités de « réidentification » existent cependant, à partir de la chaîne des transactions ou de données comme les cookies et l'adresse IP originelle¹. Des blockchains comme Bitcoin peuvent ainsi ne pas être assez anonymes, contrairement à l'argent liquide, puisque les transactions sont traçables. C'est d'ailleurs cet objectif de traçabilité – et la lutte contre la fraude qu'il permet – qui sous-tend la disparition de l'argent liquide engagée dans certains pays. Certaines blockchains sont plus anonymes que la Bitcoin et permettent des transactions illégales, pour qui sait effacer ses traces. C'est tout l'enjeu de concilier – comme avec l'argent liquide – les attentes légitimes d'anonymat, pour la protection de la vie privée ou le secret des affaires, et les objectifs de traçabilité pour lutter contre la fraude. Des outils d'analyse commencent à se développer, par exemple à

¹ Goldfeder S., Kalodner H., Reisman D. et Narayanan A. (2017), « [When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies](#) », août.

Princeton, qui permettent de tracer les opérations par-delà le pseudonymat des transactions¹.

Ces problématiques sont amenées à évoluer. Des techniques cryptographiques permettant de masquer plus ou moins complètement les transactions et les participants sont notamment mises en œuvre par les blockchains Monero et ZCash. Cette dernière utilise les techniques dites de « preuve à divulgation nulle de connaissance » (*zero knowledge proof* ou ZKP), qui sont capables d'attester la validité d'une transaction sans divulguer le montant ou l'identité des parties prenantes.

Les efforts de R & D et le foisonnement des projets en cours, annoncés ou à venir – le récent projet associé à Telegram est perçu par les spécialistes comme très prometteur – font penser que les performances et la qualité des blockchains vont être sensiblement améliorées. Les questions de gouvernance et d'interopérabilité devront aussi trouver des solutions satisfaisantes pour que la diffusion s'opère.

Derrière ces questions techniques, on retrouve très vite la dimension monétaire. Force est de constater qu'en l'état actuel des choses, les cryptomonnaies ne remplissent que très imparfaitement les trois fonctions traditionnellement dévolues à la monnaie : la volatilité de leur cours en fait des réserves de valeur incertaines ; elles ne sont pas des unités de compte, très peu de contrats usuels étant libellés en cryptomonnaies ; enfin, leur rôle de moyen d'échange reste limité par une volatilité très forte. Les cryptomonnaies sont actuellement utilisées surtout à des fins spéculatives, pour échapper aux réglementations sur le contrôle des capitaux ou pour des transactions illicites et peu à des fins commerciales licites².

Les applications monétaires des cryptomonnaies sont par ailleurs limitées par les caractéristiques intrinsèques des dispositifs sous-jacents. Le pseudo-anonymat offert par les cryptomonnaies, la spécificité des règles de validation des transactions et l'absence de valeur des cryptomonnaies en dehors du dispositif qui les supporte empêchent souvent un interfaçage direct des blockchains entre elles³, ainsi que des blockchains avec les systèmes de règlement traditionnels en monnaie traditionnelle.

¹ Kalodner H., Goldfeder S., Chator A., Möser M. et Narayanan A. (2017), « [BlockSci: Design and applications of a blockchain analysis platform](#) »,

² Voir en particulier Foley S., Karlsen J. R. et Putnîș T. J. (2018), *op. cit.* ; « Payment adoption of Blockchain tech seems more imminent than cryptocurrency » (2018), in *Decrypting Cryptocurrencies: Technology, Applications and Challenges*, J.P. Morgan Perspectives, Global Research, 9 février ; et Banque de France (2018), *Focus* n° 16, *op. cit.*

³ Des projets d'« [atomic swaps](#) » sont en cours pour rendre possible des transactions pair-à-pair entre deux chaînes différentes.

L'incapacité des cryptomonnaies à s'interfacer sans risque avec le monde réel (autres monnaies, comptes bancaires, systèmes de paiement) pour dénouer des opérations de bout en bout est aujourd'hui une limite majeure pour le développement de l'Internet de la valeur. Cette question de l'interface avec le monde physique et des fluctuations de valeur n'est toutefois pas rédhibitoire pour tous les usages. Certains usages peuvent d'ores et déjà s'en accommoder comme les jeux en ligne, qui s'inscrivent dans une temporalité limitée, ou les transferts de fonds internationaux susceptibles d'être plus rapides et moins coûteux avec une blockchain qu'avec les organisations techniques existantes.

Pour autant, le plein développement de l'Internet de la valeur nécessitera la capacité à supporter des transactions de bout en bout entre les blockchains et la monnaie quotidienne. Une des modalités pour y parvenir consisterait, comme on va le voir dans le chapitre suivant, à créer une monnaie digitale de banque centrale, interfaçable avec les dispositifs existants.

Conclusion

Ceux qui sont plus sensibles aux promesses qu'aux obstacles de la blockchain n'hésitent pas à prédire une profonde mutation à la fois économique, sociale et politique, où la confiance l'emporterait sur la défiance, l'horizontalité sur la verticalité, la décentralisation sur la centralisation. À dire vrai, la révolution annoncée ne s'est pas encore produite, malgré les milliers de projets en développement.

Cette arrivée à maturité pourra prendre du temps. **Il ne faut pas attendre pour autant et s'engager résolument. Certaines des objections évoquées ci-dessus ne s'appliquent pas aux Blockchains privées ou permissionnées, qui sont évolutives. Quant aux blockchains publiques, c'est en les testant et en les faisant évoluer qu'on en améliore la performance. Plus généralement, on sait que dans l'économie numérique les effets de réseaux sont tels que les entreprises trop attentistes, celles qui pensent trop à préserver leurs situations acquises, risquent de se trouver exclues ou marginalisées.**

Face à cette montée en puissance progressive, quelle doit être l'attitude des pouvoirs publics ? Sous prétexte de ne pas brider l'innovation, peuvent-ils ne pas s'impliquer dans les usages d'une technologie dont le potentiel est aussi puissant qu'à double tranchant ? En deçà des grands rêves de mutation anthropologique, ce sont les enjeux de politique publique qui nous intéressent ici.



CHAPITRE 4

LES POUVOIRS PUBLICS ENTRE SOUTIEN À L'INNOVATION ET RÉGULATION

Face à une technologie qui revendique volontiers son inspiration anti-étatique et qui intéresse de plus en plus d'acteurs politiques et économiques, petits comme grands, les pouvoirs publics sont naturellement hésitants, pour ne pas dire davantage. Les expérimentations se multiplient. Les bogues, les dérives frauduleuses ou criminelles, et donc la nécessaire protection des investisseurs comme des consommateurs, fournissent les raisons d'une intervention croissante. Une chose est sûre : personne ne veut rater le coche d'une possible révolution. L'idée d'une régulation fait ainsi son chemin chez la majorité des acteurs.

1. Un intérêt mondial

L'attitude à l'égard des cryptomonnaies varie d'un pays à l'autre. La tentation du contrôle est notamment perceptible en Asie. Un article publié en janvier 2018 dans *The Economist* résume la variété des politiques menées en matière de crypto-actifs par le Japon, la Chine et la Corée¹. Le gouvernement chinois, très intéressé par la technologie, conduit actuellement une politique restrictive à l'égard des cryptomonnaies : « *Last year China banned domestic exchanges ; in recent days it has taken aim at websites flouting this ban. Officials have also called on local authorities to choke off the power supply to bitcoin miners, computer networks that create new coins through massively energy-intensive calculations. China's miners, still dominant in the global industry, are shifting to other countries.* » Pour autant, l'information selon

¹ *The Economist* (2018), « [The crypto sun sets in the East: The threat of tough regulation in Asia sends crypto-currencies into a tailspin](#) », 18 janvier.

laquelle la banque centrale de Chine réfléchirait à la mise en place d'une monnaie virtuelle nationale est toujours d'actualité¹.

Le gouvernement japonais, lui, a adopté une loi sur les cryptomonnaies qui laisse une place au développement et légalise le paiement, mais dans un cadre contrôlé. Quant au gouvernement coréen, il est en train de mettre en place une politique de contrôle strict, après une vague spéculative exceptionnelle dans un cadre très ouvert.

Cette divergence asiatique se retrouve au niveau mondial sur la réglementation des ICO. Dans un article très complet, le juriste Stephane Blemus analyse les cadres réglementaires donnés à la blockchain à travers le monde, et conclut ainsi : « *As of today, mainly official positions, public reports and “soft law” decisions have been published worldwide, searching a fine line between investor protection and economic attractiveness of the local country. Few “hard law” legislations and few court rulings are to be counted. Uncertainties remain as to the legal and economic qualification of virtual currencies, tokens, ICOs, smart contracts and distributed ledger technology.* »²

Les différences de politiques s'accompagnent en tout état de cause actuellement d'une volonté accrue, dans les pays les plus développés, de contrôle des pratiques frauduleuses, blanchiment, financement du terrorisme³, arnaques, etc. En témoigne la mise à l'ordre du jour du G 20 du sujet, à la demande de la France.

Par ailleurs, tous les « grands » pays ont d'ores et déjà affiché un intérêt marqué pour la technologie (États-Unis, Royaume-Uni, Chine, Japon, Corée, Russie, Allemagne, etc.). Des stratégies nationales spécifiques se font jour dans des plus petits pays comme la Suisse, l'Estonie ou Dubaï : elles sont orientées sur l'attractivité du pays à l'égard des start-ups pour la Suisse ou sur le développement de services publics pour l'Estonie ou Dubaï. Enfin, du côté des industriels, quelques acteurs comme IBM cherchent à se positionner dans le développement de solutions. Pour l'instant les grands acteurs des plateformes numériques sont plutôt restés en retrait⁴.

¹ Voir DG Trésor (2017), « [Eessor des monnaies virtuelles en Chine : les autorités entre défiance et accompagnement](#) », 26 octobre. Tout en affichant sa prudence, le gouverneur de la Banque centrale chinoise annonçait encore récemment un programme de test en matière de cryptomonnaies (*The China Daily*, 3 mars 2018).

² Blemus S. (2017), « [Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide](#) », *Revue trimestrielle de droit financier*, n° 4-2017, décembre.

³ Politique de connaissance des clients (*Know Your Customer* ou KYC) et de lutte contre le blanchiment (*Anti-Money Laundering* ou AML).

⁴ Mark Zuckerberg, PDG de Facebook, a annoncé cependant en faire un de ses sujets de travail pour 2018.

2. L'expérimentation par les banques centrales et les réflexions en cours

Ces derniers mois est apparu dans l'actualité un sujet à haute valeur stratégique, la création d'une monnaie numérique de « banque centrale ». L'idée serait à l'étude au Royaume-Uni, au Canada, en Inde, en Suède, en Chine, à Singapour et en Russie. Le Venezuela a même lancé en février dernier le « Petro ». Des travaux non seulement techniques mais aussi économiques sont en cours dans plusieurs pays.

Deux économistes de la Banque des règlements internationaux (BRI) ont fait paraître en septembre 2017 leur étude sur les formes possibles de cryptomonnaies émises par une banque centrale¹. Les économistes de la Banque d'Angleterre et de la Banque d'Australie ont récemment prolongé la réflexion en l'accompagnant d'un appel au débat². Aucune de ces contributions n'engagent bien sûr leurs institutions mais le débat est bel et bien lancé. Un nouvel acronyme a même vu le jour, CBDC, pour Central Bank Digital Currency.

Les articles précités mettent en évidence l'impact variable, mais contrôlable, que serait susceptible d'avoir une telle transformation sur le système bancaire actuel, puisque les particuliers pourraient dans certains scénarios détenir directement de la monnaie numérique banque centrale, sans passer par l'intermédiaire d'une banque. Quand les particuliers n'y ont pas accès et qu'il y a seulement un marché de gros accessible au système bancaire, l'impact est cantonné. En tout état de cause, les risques semblent limités et contrôlables pour les États et l'adaptation de la politique monétaire par les banques centrales ne semble pas poser de problème majeur. Christian Pfister a publié en 2017 un article sur la politique monétaire associée à une monnaie virtuelle qu'il conclut ainsi³ : « L'usage des monnaies digitales ne pourrait très vraisemblablement se répandre que dans des conditions qui laisseraient foncièrement inchangées la capacité de la banque centrale à poursuivre un objectif d'inflation identique par les mêmes moyens que de nos jours, en fixant un niveau de taux d'intérêt. Cependant, quelques ajustements pourraient devoir être apportés à la définition des agrégats monétaires ainsi éventuellement qu'à la base et/ou aux ratios de réserves obligatoires. Même dans le cas extrême et très improbable où de la

¹ « Central bank cryptocurrencies », Morten Bech et Rodney Garratt, BIS Quarterly Review, September 2017

² Kumhof M. et Noone C. (2018), « [Central bank digital currencies – design principles and balance sheet implications](#) », Staff Working Paper n° 725, mai.

³ Christian Pfister (2017), « Monnaies digitales et politique monétaire : beaucoup de bruit pour rien ? », *Revue française d'économie*, 2017/2, Vol. XXXII, p. 37-63.

monnaie digitale de banque centrale avec des attributs de dépôt serait émise et où le public l'adopterait massivement, le rôle des banques dans la distribution de crédit, bien que s'exerçant dans des conditions plus difficiles en raison d'une moindre information directe sur leur clientèle, ne devrait pas être gravement compromis. Les banques deviendraient plutôt fortement dépendantes du refinancement de banque centrale, ce qui militerait pour l'annonce d'une politique de prêteur en dernier ressort fondée sur des règles afin de limiter le risque moral (Pfister et Valla, 2017). Les banques ne disparaîtraient que dans le cas limite de "socialisme financier" (Raskin et Yermack, 2016). Cependant, la décision de poursuivre une telle voie serait hautement politique et ne serait pas forcément acceptée par le public. »

Ces contributions scientifiques ont été complétées par un rapport beaucoup plus institutionnel de la BRI qui, avec toute la prudence propre aux institutions financières, prolonge les réflexions ci-dessus¹. En mars 2018, le Comité sur les paiements et les infrastructures de marché, qui fonctionne dans le cadre de la BRI, estime que le potentiel est immense dans les paiements interbancaires, la compensation et les règlements, tout en mettant en garde les banques centrales sur les « implications pour la stabilité financière et la politique monétaire de l'émission de monnaies digitales accessibles au grand public ». Son très récent rapport annuel prolonge cet appel à la prudence.

3. Vers la régulation ?

La disjonction entre la blockchain et les cryptomonnaies a permis de confirmer les potentialités de la technologie et de ne pas brider l'innovation. Les projets se multiplient, qui mobilisent le « registre distribué » sans nécessairement recourir à une monnaie virtuelle. Force est cependant de constater aujourd'hui que les blockchains sont difficilement séparables de ce qu'on les appelle les jetons et les cryptomonnaies (voir en fin de volume la contribution du groupe de travail intitulée « Les enjeux juridiques de la blockchain », fiche 1, sur l'analyse juridique des « *tokens* »).

En septembre 2017, l'intervention de la présidente du FMI Christine Lagarde devant les banquiers centraux témoigne de cette convergence. Elle les a incités à intégrer les monnaies virtuelles dans leur réflexion stratégique : « Les monnaies virtuelles telles que Bitcoin ne présentent actuellement peu ou pas de danger pour le régime existant de monnaies fiduciaires et de banques centrales. Elles sont en effet trop volatiles, trop risquées, trop compliquées à utiliser, et les technologies sous-jacentes

¹ Central bank digital currencies, Report submitted by Working Groups chaired by Klaus Löber (European Central Bank) and Aerdts Houben (Netherlands Bank), mars 2018.

ne peuvent pas encore être déployées à grande échelle. Un grand nombre d'entre elles sont trop obscures pour les autorités de réglementation, et plusieurs ont déjà été piratées. Mais ces problèmes sont principalement d'ordre technologique et pourraient être réglés à terme. Il n'y a pas si longtemps, des experts déclaraient que les ordinateurs personnels n'avaient aucun avenir ou que les tablettes n'étaient que de coûteux gadgets. Il me semblerait donc imprudent de ne pas prendre les monnaies virtuelles au sérieux (...) Elles pourraient par exemple être émises à parité avec le dollar, ou rattachées à un panier stable de devises. Leur émission pourrait être totalement transparente et régie par une règle crédible et prédéterminée, un algorithme qui peut être surveillé... ou même par une "règle intelligente" qui pourrait s'adapter à l'évolution de la conjoncture macroéconomique. »

Le message est fort : une fois passé la phase de mise au point, cette technologie est susceptible de bouleverser l'économie. Les échanges devenus par ailleurs totalement numérisés pourraient être certifiés grâce à la blockchain. De plus, les opérations entourant les échanges (appels d'offres, validation partielle par des tiers, règlements conditionnés, etc.) pourraient être gérés automatiquement et en confiance grâce aux *smart contracts*. En somme, l'économie deviendrait en partie programmable.

En France, depuis quelques années, plusieurs acteurs institutionnels majeurs – Assemblée nationale, Consortium LabChain autour de la CDC, Banque de France, AMF, Trésor, MEDEF – ont porté des initiatives montrant leur volonté de favoriser le développement des blockchains en France¹ et de ne pas réglementer trop vite. Un écosystème dynamique a commencé à se développer avec des startups cartographiées par BPI France (voir tableau 2 ci-dessous), des cabinets de conseil et l'implication de grandes entreprises qui étudient le sujet et y dédient des ressources. Cet écosystème s'appuie sur une communauté de passionnés d'origine diverse, où les spécialistes de l'informatique, de la cryptographie et de l'algorithmique côtoient ceux de la finance, de l'économie, du droit, de l'histoire, etc. Les spécialistes français du sujet se sont d'ailleurs regroupés (la « Communauté » comme ils se dénomment eux-mêmes) autour d'organisations de passionnés, de toutes origines disciplinaires et professionnelles, extrêmement dynamiques. Le Cercle du Coin, « Association francophone sur le Bitcoin, les monnaies décentralisées et les blockchains » en est probablement le plus emblématique.

¹ Lab de la CDC, projet Madré de la BdF, conférence au Parlement, débat législatif, loi Sapin 2 introduisant les minibons, consultation de l'AMF...

Tableau 2 – Une cartographie de la blockchain en France

Infrastructure & Protocol	Applications			Consultancy & Services
Blockchain	Energy	Fintech / payment	Marketplace / retail	General practitioners
• Tezos(OcamlPro)	• Daisee • Enerfip • Evolution Energy • Lumo • Petroleum-project • Solarcoin/ Ekwater • Sunchain	• Hipay • La Maison du bitcoin • Limonetik • Moneytrack • Utocat	• Dawex • Ledgys • Mubiz • Sandblock.io	• Blockchain Partner • Blockchain Solutions • Blockchain Strategists • Cellabz • Kingiri • Mezzonomy • Startuptoken • U (Uchange.Co)
Scalability			Wallet	
• Acinq • Tresoriomining		Exchange	• Czam • Goochain (Citadelle) • Ledger	Fintech
Middleware	Govtech	• Paymium • Dether	Supply Chain	• Belem
Dev/Tech	• CommonAccord (Cmacc Transact)	Security	• Connecting Food • Makernet • Playitopen • Seezart • Tilkal	IoT
• Deepblock • Stratumn	Legal	• Blockchain Inspector • Blockshare • Chainhero • Tanker • Ugloo • Uniris • Woleet	Mobility	• ChainOrchestra • Fablaboo
Distributed computing	• BlockchainyourIP • Openflow • Magush • Keeex • Evoluchain		• Pack And Drive	Media / Training
• iExec • Rockchain	Games	Healthtech	Insurtech	Supply Chain
Identity & Privacy	• Beyond the void	• Kidner project	• Wekeep	• Crystalchain
• Matchupbox				

Source : Le Hub-Bpifrance, novembre 2017

Après une période où la régulation semblait l'ennemi juré de l'innovation, l'heure semble venue de trouver un moyen de tenir la chaîne par les deux bouts : réglementer de façon coordonnée sur un certain nombre de sujets permettra à la fois de contrôler les usages délictueux et de favoriser les développements souhaités.

À ce stade du développement des usages, l'insécurité juridique sur des sujets de base comme la comptabilité, la fiscalité ou la relation avec les banques et le manque d'expertise des pouvoirs publics deviennent néfastes, tant du point de vue du contrôle des usages délictueux que de l'accompagnement du développement industriel d'un secteur prometteur.

Les acteurs de ces développements ont pour la plupart acquis des cryptomonnaies dans le cadre de leurs activités, ce qui les place aujourd'hui dans une insécurité juridique majeure, sur un plan comptable autant que fiscal (voir la contribution sur les enjeux juridiques en fin de volume). Aujourd'hui, faire une ICO « légale », comme l'envisage l'AMF au travers de sa consultation publique, suppose nécessairement de lever de la cryptomonnaie, alors que les modalités d'enregistrement comptable d'une cryptomonnaie ne sont pas précisées, ce qui peut conduire à enregistrer les ressources hors bilan et à fragiliser cette entreprise.

Quant aux particuliers détenteurs de cryptomonnaies, l'absence de régime spécifique aux plus-values semble conduire à leur appliquer un régime fiscal extrêmement défavorable – avec un taux maximum de 62 % –, y compris au regard des pratiques de plusieurs pays comparables (voir tableau 3). Certes, une décision récente du Conseil d'État apporte un correctif à cette situation, mais en répondant à des requérants qui demandaient l'annulation de commentaires administratifs de 2014, elle s'avère donc partielle¹. En contrepartie d'exigences de transparence, comme celles que sont en train de mettre en place plusieurs pays (États-Unis, Australie), l'application d'une fiscalité similaire à celle d'actifs plus classiques pourrait être envisagée. Cette politique conduirait sans doute à ne pas créer de nouvelles poches d'évasion fiscale ou d'exil fiscal.

**Tableau 3 – Taux d'imposition comparé des plus-values
sur les gains en cryptomonnaies pour les particuliers**

État	Taux d'imposition
Allemagne	Imposition au titre des plus-values privées au taux de 25 %
États-Unis	Régime des plus-values à long terme : application d'un taux marginal de 20 %
Israël	Imposition au titre des plus-values privées au taux forfaitaire de 25 %
Italie	Pas d'imposition en l'état de la réglementation
Royaume-Uni	Imposition pour un investisseur au taux forfaitaire de 28 %

Source : contribution du groupe de travail « Les enjeux juridiques de la blockchain »

En parallèle de ces mesures de clarification réglementaire, des mesures favorables au développement des blockchains doivent être mises en place. Le sous-rapport « Les enjeux juridiques de la blockchain » qui figure en fin de volume analyse des sujets pour lesquels des évolutions législatives ou réglementaires sont possibles à court terme. Les solutions envisagées soutiendraient et sécuriseraient les investissements en répondant à l'insécurité juridique par des solutions attractives et incitatives au développement et à l'innovation.

En matière de recherche, les limites actuelles des blockchains méritent des travaux de recherche, notamment sur la question de la scalabilité, de la consommation

¹ Conseil d'État, 26 avril 2018, *M. G...et autres*, Nos 417809, 418030, 418031, 418032, 418033.

d'énergie, de l'interopérabilité entre les chaînes, de la gouvernance ou de la robustesse des *smart contracts*.

Il va falloir, après la phrase des démonstrateurs (POC), sortir du bac à sable pour ne pas être dépassé par des stratégies privées ou frauduleuses, mais avec prudence, pour ne pas laisser le ver dans le fruit. Il est temps d'introduire les régulations de base qui soutiendront et sécuriseront l'investissement et les compétences. Ces mesures concernent les champs fiscaux, comptables, juridiques, de sécurité publique, qui doivent être coordonnés pour préserver les incitations des acteurs tout en cherchant à bloquer les initiatives dangereuses.

Quatre objectifs simultanés doivent donc être poursuivis :

- la protection de l'investisseur ;
- la protection de l'entrepreneur ;
- la protection de l'utilisateur/consommateur/épargnant ;
- la garantie de l'ordre public.

Conclusion

Il conviendrait d'instituer à l'intérieur de l'État un groupe qui apporte des réponses coordonnées et équilibrées aux questions réglementaires soulevées par les blockchains, en matière de fiscalité, de droit au compte, de lutte contre le blanchiment et de traitement comptable, et qui dispose de l'appui technique nécessaire à un tel travail. Au-delà de ces mesures, il est nécessaire de construire les infrastructures blockchains publiques de demain. Deux scénarios sont envisageables : ou bien encadrer suffisamment les blockchains existantes ; ou bien favoriser le développement de nouvelles infrastructures plus sécurisées. À ce jour, il est difficile de trancher le dilemme : le rapport recommande donc de mener de front les deux stratégies de « maîtrise » des blockchains existantes et d'accompagnement de l'émergence de nouvelles solutions.



CHAPITRE 5

RECOMMANDATIONS

Le groupe de travail formule ici sept recommandations qui doivent être considérées comme de premières orientations au niveau national. Comme pour tout ce qui a trait au numérique, la dimension européenne est éminemment nécessaire, en particulier pour les questions relatives au droit de la preuve ou à la comptabilité. En réalité, en matière de blockchains, c'est une réponse à l'échelle mondiale qu'il convient de viser si on veut lutter efficacement contre le blanchiment d'argent ou la fraude. La Commission européenne et le Parlement européen ont engagé des travaux de réflexion ainsi que différentes initiatives, et des financements sont prévus dans le cadre du programme H2020¹.

1. Promouvoir des travaux de recherche et développement en misant sur l'interdisciplinarité

Contrairement à ce que l'on observe dans les processus classiques de R & D, la Blockchain n'est pas née dans des laboratoires de recherche ou dans une université. Les différentes composantes de cet assemblage ont certes vu le jour dans des environnements académiques, mais le protocole Bitcoin a été développé à partir d'un article posté sur une liste de diffusion². L'engouement académique pour cette technologie est d'autant plus récent qu'une bonne recherche nécessite la mise en place d'équipes multidisciplinaires, ce que les modes d'organisation à la française – essentiellement disciplinaires – ne favorisent pas.

¹ La Commission européenne vient de créer son observatoire-forum des chaînes de blocs, confié à l'entreprise ConsenSys (voir « La Commission européenne lance l'Observatoire-forum des chaînes de blocs de l'UE », communiqué de presse du 1^{er} février 2018). Elle a par ailleurs lancé un concours visant à favoriser le développement d'applications efficaces au service de l'intérêt général.

² Les premiers textes publiés dans des revues semblent avoir été écrits fin 2011 et publiés en 2012 (Google Scholar).

Inria, organisme public de recherche dédié au numérique, a retenu les quatre domaines théoriques suivants : la formalisation, la sécurité (intégrité, confidentialité, preuves, opposabilité), la qualité de service (bande passante, latence, robustesse, fiabilité) et enfin la gouvernance (évolution, neutralité)¹.

Ces travaux de R & D devraient permettre de progresser sur des questions souvent mises en avant, comme l'impact écologique du protocole de consensus, la protection des données personnelles, l'identité numérique ou l'interopérabilité entre chaînes. En tout état de cause, un programme national pluridisciplinaire devrait être lancé.

2. Inciter au développement de formations approfondies et favoriser l'appropriation du sujet

Comme toujours, R & D et formations doivent aller de pair. Les tout premiers cursus diplômants commencent à apparaître à France, mais force est de constater que nous sommes en retard, à l'exception du pôle universitaire Léonard de Vinci qui a fait figure de précurseur avec un premier cours en 2015. Aux États-Unis, les plus grandes universités – et pas seulement elles – proposent des formations (Berkeley, Stanford, Princeton, le MIT, Duke, New York University, etc.). Princeton a mis en place un MOOC réputé depuis 2015. Rien ne justifie que les universités françaises comme les grandes écoles d'ingénieurs – dont l'une des spécificités est la capacité à conceptualiser et à combiner des disciplines scientifiques – ne fassent pas de même. Développer des projets innovants suppose de comprendre les concepts sous-jacents et pas seulement de coder dans tel ou tel nouveau langage. En l'occurrence, ce n'est pas si simple car les blockchains se fondent sur de la cryptographie, de l'algorithmique, de l'économie des incitations, des réseaux pair-à-pair et de l'informatique distribuée. L'objectif de formation pour participer au développement des systèmes blockchain doit aller au-delà de la nécessité de former de (bons) développeurs. Il s'agit d'aider à l'appropriation de systèmes complexes, condition nécessaire au développement.

L'effort de formation ne doit pas se cantonner aux spécialistes. L'enjeu central sera le développement des usages. L'expérience montre qu'il suppose la compréhension des métiers et des applications pour lesquels l'utilisation des protocoles Blockchain est intéressante. Or la compréhension du sujet nécessite un investissement personnel fort qui doit être facilité, dans les institutions concernées, par des

¹ Inria (2018), *Plan stratégique scientifique*, mars. Voir le « défi scientifique n° 8 » intitulé « Des systèmes distribués sans autorité centrale ».

investissements significatifs pour former les acteurs de ces transformations et les impliquer. Cet effort concerne aussi les administrations (voir recommandation 6).

3. Établir les régulations de base pour contrôler les usages frauduleux des cryptomonnaies et développer les usages des blockchains en s'appuyant sur un groupe à compétences transversales, à l'intérieur de l'État

Sur un certain nombre de sujets, il y a urgence à ce que l'État apporte des réponses coordonnées et équilibrées en vue des objectifs concomitants de soutien à l'innovation et de préservation de l'ordre public. Il faut disposer de l'appui technique nécessaire à la définition de solutions efficaces et répondre sans tarder aux différentes questions réglementaires soulevées en matière de fiscalité, de droit au compte, de lutte anti-blanchiment et de traitement comptable.

Pour laisser la place à la créativité, il convient d'instituer des régulations de base qui soient raisonnablement attractives : c'est une nécessité pour soutenir les applications légales. La philosophie générale consiste à mettre en place les règles minimales efficaces, tout en conservant les caractéristiques de simplicité des dispositifs actuels¹. Cette démarche correspond de fait à celle de l'AMF en matière d'ICO (cf. supra). En tout état de cause, les initiatives doivent s'inscrire dans un mouvement international, initié par la réunion du G20 de mars 2018, qui a demandé un rapport sur la question pour juillet 2018².

Les points suivants nous paraissent prioritaires :

- se donner davantage de moyens techniques et humains pour lutter contre les usages frauduleux ; définir et contrôler les règles de *reporting* applicables aux places de marché (exchanges), en développant des outils d'analyse, comme cela a été fait à Princeton sur le traçage des transactions ;
- clarifier les règles fiscales et comptables qui protègent l'entrepreneur, l'investisseur et l'ordre public ; être capable de les adapter régulièrement en fonction des évolutions technologiques ;

¹ Les spécialistes étant souvent possesseurs de bitcoins et autres cryptomonnaies, il peut y avoir des conflits d'intérêt.

² Voir le [communiqué de presse](#) du G20, 20 mars 2018.

- définir les règles spécifiques qui permettraient aux entreprises actives dans les cryptomonnaies de respecter leurs obligations de KYC et AML permettant d'assurer un droit effectif au compte.
- accompagner l'AMF à propos des ICO et faire avancer la réflexion sur le statut juridique des jetons ;
- clarifier la valeur de preuve d'une inscription sur une blockchain.

Après une période où il fallait laisser se déployer toutes les initiatives pour faciliter l'innovation, les inconvénients de l'insécurité juridique prennent le pas sur les avantages. Nous avons identifié un certain nombre de sujets sur lesquels la mise en place d'une réglementation ou de règles *ad hoc* au moins provisoires – à réévaluer ultérieurement – apparaît souhaitable : questions fiscales et comptables, jetons, accès effectif au compte pour les entreprises, preuve. L'analyse de ces sujets est réalisée dans un « sous-rapport juridique » qui résulte du travail d'un groupe spécifique de participants réunis par France Stratégie (voir la contribution « Les enjeux juridiques de la blockchain, en fin de volume).

Le parti pris de ce complément juridique n'est pas de faire l'état des lieux de toutes les questions auxquelles sont confrontés les juristes pour intégrer les apports potentiels des blockchains dans les caractéristiques des services offerts. Les difficultés sont nombreuses dans la mesure où tous les mécanismes traditionnels de certification et de validation des personnes, des actes et des transactions se trouvent bouleversés. Certains problèmes pourraient trouver des solutions techniques (les données personnelles ou la qualité des programmes, par exemple).

Le sous-rapport juridique traite uniquement des sujets qui doivent et peuvent à court ou moyen terme trouver des solutions pour faciliter l'objectif stratégique de soutien à l'innovation et plus particulièrement de participation active à l'utilisation des blockchains. Cela pourrait conduire à une évolution profonde des formes de traitement, de stockage et de conservation de l'information et des transactions. On trouvera dans cette contribution des éléments aussi précis que possible pour évaluer les problèmes et explorer des pistes de solutions.

Le contrôle de l'utilisation frauduleuse des cryptomonnaies est évidemment un point central, qui n'a pas fait l'objet d'un examen spécifique pour ce rapport. En tout état de cause, il est indispensable de faire en sorte que les blockchains ne drainent pas les usages frauduleux et que le niveau de contrôle obtenu via les blockchains soit au moins égal à celui du système bancaire traditionnel.

4. Contribuer au financement des projets d'infrastructure logicielle

5. Soutenir des secteurs correspondant à des domaines d'excellence ou d'intérêt stratégique en France

Rien n'indique que les *startups* du secteur des blockchains rencontrent des difficultés spécifiques à se financer en comparaison d'autres secteurs d'activité. Certaines ont même pu ou pourraient bénéficier de deux avantages qui facilitent leur financement. D'une part, l'acquisition initiale de bitcoins ou d'ethers (plus récemment d'autres cryptomonnaies), dont les valorisations ont considérablement augmenté (en tendance), a permis à certaines de se financer sur ces gains. D'autre part, les ICO permettent théoriquement d'accéder beaucoup plus aisément à un financement que les levées de fonds traditionnelles. Jusqu'à présent, les ICO ont été essentiellement utilisées par des acteurs du secteur, bien que de manière limitée en France¹.

Comme en témoigne la recension réalisée par BpiFrance, peu de startups développent des projets « d'infrastructure » en France (voir la cartographie dans le chapitre 4). La notion d'infrastructure ne renvoie pas à des infrastructures de type télécoms, puisque c'est le réseau internet qui est utilisé pour transmettre les transactions, mais à des réseaux de logiciels distribués sur des ordinateurs ou des serveurs dédiés. Plus hypothétiques, plus risqués et sans participation de grandes entreprises, les financements semblent ici plus difficiles. Pourtant, l'incertitude sur les solutions techniques qui prévaudront demain et l'importance des enjeux justifieraient une stratégie volontariste de soutien à de tels projets, couplée éventuellement aux efforts de R & D.

En ce qui concerne les secteurs à privilégier, les liens techniques et commerciaux à tisser avec des entreprises locales pour développer des applications à base de blockchains justifient de s'appuyer sur des activités d'excellence française.

Une de ces applications consiste à contrôler les chaînes d'approvisionnement, ce qui pourrait concerner par exemple l'agroalimentaire. Les registres distribués peuvent en effet contribuer à traiter ces questions en organisant un partage d'information limité et résistant à la manipulation des parties. La bonne gouvernance de ce type de réseau est une condition du succès, dans la mesure où elle doit inciter les acteurs à inscrire

¹ L'étude d'EY évalue l'usage des ICO par des entreprises basées en France à 12 millions de dollars sur un total de 4 milliards de dollars. Cf. « EY research: initial coin offerings (ICOs) », décembre 2017.

leurs données sur le système pour permettre la traçabilité. Pour autant, la confidentialité de l'information doit pouvoir être préservée pour respecter le secret commercial. Les blockchains ont la capacité de concilier ces deux objectifs en apparence contradictoire. Une architecture qui ne garantirait pas un contrôle de leurs données par les différents fournisseurs a peu de chance de fédérer effectivement l'ensemble d'une filière.

Le groupe de travail a longuement débattu de « la sortie du bac à sable ». En effet, pour l'instant, la plupart des usages ont été testés dans le cadre de POC (*Proof Of Concept*). L'idée, mise en œuvre au Royaume-Uni en particulier pour les FinTech, a consisté à réaliser des « POC » dans un environnement réglementaire favorable, baptisé « bac à sable » (*sandbox*)¹. Mais de véritables applications commencent à émerger. Dans le numérique, les effets de réseau sont extrêmement rapides. Il faut être capable de saisir les opportunités, ce qui conduit à recommander d'appuyer le développement de solutions opérationnelles, pas simplement de démonstrateurs.

6. Tester, expertiser, former et s'équiper au sein des pouvoirs publics ; analyser l'évolution des blockchains publiques ; diffuser l'information, développer et utiliser des applications non critiques

Les blockchains posent des défis originaux aux pouvoirs publics, notamment en matière de fiscalité, de comptabilité, de droit de la preuve... Plusieurs institutions publiques ont engagé des démarches pour comprendre ces enjeux et y apporter des réponses dans leur champ de compétences – AMF, Banque de France, Direction générale du Trésor, CDC, AFNOR, INPI – mais elles ne disposent pas toujours des compétences nécessaires en interne et ne peuvent embrasser toutes les dimensions simultanément. D'autres institutions publiques peuvent être concernées par les blockchains mais sans avoir développé d'expertise. En outre, comme souvent dans le domaine numérique, il est nécessaire de développer soi-même des applications pour se rendre compte des problèmes rencontrés et y répondre de façon appropriée.

Il serait donc nécessaire de créer une cellule d'agents publics ayant une expertise dans le domaine des blockchains, capables d'intervenir en appui des services de l'État. Cette cellule, de quelques agents au départ, aurait plusieurs missions :

¹ L'idée de ce genre de dispositifs est que l'État définit en bilatéral avec des entreprises candidates des conditions réglementaires « favorables » pour que ces entreprises testent une nouvelle technologie ou un nouveau mode de gouvernance, etc.

- conduire des travaux d'analyse des blockchains publiques pour développer une capacité d'expertise indépendante sur les réseaux pair-à-pair, les registres et les transactions ;
- former les acteurs publics au fonctionnement des blockchains et les aider à en appréhender le potentiel ;
- tester et développer ou faire développer des applications non critiques pour la puissance publique : parmi les sujets envisageables, on peut mentionner le stockage et la gestion de bases de données publiques ou la mise à disposition d'un système de vote par blockchain pour les collectivités et les institutions publiques ;
- diffuser l'information sur les blockchains et sur l'écosystème des acteurs français ayant fait des développements logiciel, des ETI aux startups. Les petites organisations ont plus de difficultés à accéder à la commande publique alors que la jeunesse du marché et des offres ne justifie pas que les grandes organisations bénéficient d'un avantage structurel.

7. Répondre aux défis auxquels se heurte aujourd'hui l'internet de la valeur, ce qui suppose une monnaie numérique stable

Après exposé des arguments, le besoin est avéré pour tirer parti des possibilités des transactions programmables. Des projets existent. Il vaudrait mieux pour notre souveraineté que des réponses moins contrôlables ne soient pas fournies par des acteurs privés ou par des acteurs publics étrangers.



CONTRIBUTIONS DU GROUPE DE TRAVAIL



DES RACINES LIBERTARIENNES À LA BIENVEILLANCE DU MONDE ÉCONOMIQUE : APERÇU DES IDÉOLOGIES DANS LE DÉVELOPPEMENT DES BLOCKCHAINS

par **Clément Gasull**, doctorant au Centre de sociologie
de l'innovation (MINES ParisTech) et SENSE (Orange Labs)

L'engouement suscité par « la technologie blockchain » depuis le milieu des années 2010 est à la hauteur des controverses que ses applications réelles ou projetées suscitent. Si de nombreux acteurs du monde économique (individus, institutions, entreprises) les décrivent comme révolutionnaires pour divers secteurs d'activité, d'autres dénoncent les idéologies dont elles seraient le vecteur. Pour mieux envisager l'effervescence du monde économique, nous proposons ici un aperçu des motivations idéologiques et économiques qui ont alimenté la conception de cette technologie. Nous nous sommes particulièrement appuyés sur la lecture de deux ouvrages consacrés à Bitcoin : celui d'Adli Takkal Bataille et Jacques Favier (2017)¹, promoteurs actifs de Bitcoin², et celui de David Golumbia (2016)³, chercheur en cultures numériques à l'université de Virginie (États-Unis) et critique de l'idéologie politique véhiculée par de nombreux promoteurs de Bitcoin.

¹ Takkal Bataille A. et Favier J. (2017), *Bitcoin. La monnaie acéphale*, Paris, CNRS Éditions.

² Adli Takkal Bataille et Jacques Favier sont notamment membres et co-fondateurs de l'association « [Le Cercle du Coin](#) » qui « a pour objet l'étude et la promotion des nouvelles technologies favorisant l'émergence et le développement des monnaies décentralisées et du Bitcoin ainsi que de leurs multiples applications ». L'association « se donne pour objectif d'organiser (...) la promotion et la normalisation des monnaies décentralisées auprès des autorités locales, régionales, nationales et des instances de coopération internationale. ».

³ Golumbia D. (2016), *The Politics of Bitcoin Software as Right-Wing Extremism*, Minneapolis, University of Minnesota Press.

La technologie blockchain s'est construite en opposition avec les politiques classiques d'administration de la monnaie. La première blockchain est née avec Bitcoin, décrit par son ou ses créateurs Satoshi Nakamoto comme « un système électronique d'échange de liquidités de pair-à-pair »¹. La technologie blockchain porte en elle dès sa première application le souhait de permettre aux individus d'opérer directement des transactions sans intermédiaire. Pour Nakamoto et ses premiers utilisateurs, Bitcoin répondrait à une confiance ébréchée dans les échanges monétaires, résultat d'une défiance vis-à-vis des politiques conjointes des banques centrales et des banques commerciales. Cette défiance est formulée par trois critiques de la valeur des monnaies fiduciaires d'État. Premièrement, les banques centrales dévalueraient la monnaie par des politiques inflationnistes qui impliqueraient une dévalorisation des avoirs monétaires des citoyens. Deuxièmement, les banques commerciales alimenteraient des bulles spéculatives par la création monétaire (scripturale, par l'octroi du crédit) sans pour autant disposer de réserves en liquidités suffisantes (critique du système de réserves fractionnaires). Troisièmement et en corollaire des deux critiques précédentes : la garantie d'État souverain vis-à-vis de la monnaie serait a minima insuffisante, sinon fictive². Ces critiques alimentent un procès en « fausse monnaie » des monnaies d'État : si tout actif monétaire peut perdre sa valeur sur décision d'État (première critique) sans que celui-ci n'en garantisse la valeur (troisième critique), la garantie monétaire d'État porterait sur l'usage pratique de la monnaie uniquement (a minima, celui de payer les impôts), mais pas sur la valeur d'une unité monétaire. Selon ses soutiens, Bitcoin répondrait à ces critiques grâce à son organisation horizontale et son modèle économique appuyé sur la finitude de sa masse monétaire. Déconnecté du système monétaire traditionnel, banques centrales et commerciales en particulier, Bitcoin fonctionnerait grâce à une gestion « décentralisée », « distribuée » entre les différents membres du réseau (notamment mineurs, développeurs, utilisateurs). Cette architecture participerait ainsi et selon ses promoteurs à une « administration démocratique » car indépendante d'institutions centralisées jugées non représentatives. Elle reposerait non seulement sur son mode de gouvernance, mais aussi sur la sécurité de son réseau, une multitude de nœuds indépendants ne présentant pas de point d'attaque unique (« *single point of failure* ») et sur le

¹ Nakamoto S. (2008), « [Bitcoin: A Peer-to-Peer Electronic Cash System](#) ».

² Takkal Bataille et Favier (2017) illustrent cette troisième critique en s'appuyant sur des estimations du montant capitalisé du Fonds de garantie des dépôts et de résolution et du nombre de comptes bancaires de déposants : « Quelle est la valeur de la garantie offerte en contrepartie de cette servitude bancaire [au sens des deux premières critiques] ? Faible. Celle-ci n'est pas vraiment accordée par l'État mais par un Fonds de garantie capitalisé de 3 milliards, soit une vingtaine d'euros pour chacun des 140 millions de comptes de particuliers » (p. 69).

caractère incorruptible de la base de données de transactions garantie par l'importance de la quantité d'énergie qu'il faudrait déployer pour la falsifier et induire en erreur le réseau. Enfin, elle protégerait les détenteurs de jetons des autorités qui disposent d'une part d'une capacité de saisie sur les actifs en monnaie fiduciaire¹, d'autre part d'une capacité de démonétisation de certaines liquidités². Les soutiens de Bitcoin comparent en effet les jetons Bitcoin à un « or numérique » : comme les métaux précieux en général et l'or en particulier, les jetons Bitcoin seraient ceux d'une « devise forte », valorisables « pour eux-mêmes ». Ils seraient non seulement indépendants d'une quelconque autorité souveraine et non adossés à un quelconque actif, mais aussi émis en nombre fini³. En ce sens, Bitcoin est souvent revendiqué comme une « monnaie de la finitude » à l'échelle d'un « monde fini », en opposition à des « monnaies de crédit » qui incarneraient une logique productiviste. Cette mise en œuvre canonique des blockchains qu'est Bitcoin propose un nouveau paradigme des relations de confiance pour les échanges monétaires reposant sur un réseau considéré comme puissant par son mode de gouvernance et par l'énergie nécessaire à son fonctionnement qui garantit les transactions qu'il valide, en opposition affirmée à une garantie d'État jugée incertaine. En ce sens, Bitcoin représente une critique de l'intermédiation entre les individus, dénonçant l'État souverain comme organisateur des échanges monétaires et les banques commerciales comme intermédiaires des paiements. La critique formulée par les promoteurs de Bitcoin est donc non seulement économique, à propos de la monnaie et des échanges de valeur, mais aussi politique. D'une part Bitcoin trace ou rêve un réseau et une communauté fonctionnant sans intermédiaire, d'autre part Bitcoin revendique une volonté d'anonymat et de sécurité totale des transactions⁴.

David Golumbia rappelle que les critiques formulées par les promoteurs de Bitcoin, mais aussi la plupart de ses caractéristiques techniques, se retrouvent dans différentes tentatives de solutions de paiement plus anciennes. En 1983, avant l'ère Internet, l'informaticien David Chaum a conçu ECash, un système de gestion de l'argent liquide de manière électronique permettant à un acheteur de réaliser des paiements de façon chiffrée et certifiée par une banque (la société Digicash) sans besoin ni d'ouvrir un compte chez son fournisseur ni de transmettre ses références de carte bancaire. En 1997, Citybank proposa le concept d' « Electronic Monetary

¹ L'exemple de la ponction des dépôts chypriotes de plus de 100 000 euros, en 2013, est souvent cité comme un cas d'école.

² L'Inde a décidé de démonétiser des coupures de 500 et 1 000 roupies en novembre 2016.

³ Le nombre total de jetons de Bitcoin est fixé à 21 millions, émis par le réseau au fil du temps.

⁴ Les utilisateurs de Bitcoin échangent en utilisant des pseudonymes.

System »¹ (EMS) permettant des échanges d'argent liquide sous forme électronique directement entre institutions financières. En 1998, PayPal lança sa plateforme de paiement entre personnes physiques permettant, à partir d'une adresse de courrier électronique et d'un mot de passe, des transactions en communiquant une seule fois ses coordonnées bancaires. Alors que ces tentatives impliquaient toujours des intermédiaires bancaires ou des entreprises administrant les paiements, une étape supplémentaire fut franchie en 1998 avec B-money puis en 2005 avec Bit gold. B-money et Bit gold sont respectivement un système de monnaie électronique anonyme et une proposition de monnaie électronique décentralisée, qui tous deux introduisent des notions reprises pour Bitcoin et d'autres cryptomonnaies². Leurs concepteurs, Wei Dai et Nick Szabo, respectivement ingénieur informatique et cryptographe, sont souvent associés aux mouvements cypherpunks³. Ce groupe informel de personnes intéressées par la cryptographie a pour objectif de défendre le respect de la vie privée par l'utilisation proactive de la cryptographie. Les cypherpunks dénoncent le « contrôle » des gouvernements et des grandes entreprises sur les transactions financières dans des écrits inspirés de ceux de David Chaum, comme le *Manifeste d'un cypherpunk* écrit en 1993 par Eric Hughes ou le *Manifeste crypto-anarchiste* de Tim May écrit en 1992. Les crypto-anarchistes considèrent que le développement et l'utilisation de la cryptographie sont la meilleure défense contre la surveillance des communications informatiques, notamment sur Internet. Ils dénoncent en particulier l'application de réglementations de prévention du terrorisme⁴ ou anti-blanchiment nées dans les années 2000, qui autorisent le déchiffrement d'informations chiffrées sur demande d'un juge et exigent que des intermédiaires financiers comme les banquiers identifient précisément leurs clients⁵. En réaction, les crypto-anarchistes plébiscitent l'anonymisation des données, en particulier des correspondances et des transactions, et affirment qu'une monnaie indépendante des États et des gouvernements est un idéal souhaitable. Les concepteurs et premiers utilisateurs de Bitcoin et des cryptomonnaies se rapprochent

¹ Voir « [Electronic-monetary system](#) », United States Patent 5453601..

² Notamment les principes de « preuve de travail », de partage du travail de vérification des transactions *via* un livre de comptes partagé par une communauté, de rémunération du travail par l'émission de monnaie, de tenue de compte collective authentifiée par des *hashes* cryptographiques, de signatures électroniques par « clés publiques ».

³ Deux figures emblématiques des cypherpunks sont Julian Assange – activiste luttant contre « l'asymétrie d'informations » en diffusant des câbles diplomatiques – et Philip Zimmermann – inventeur du logiciel PGP visant à rendre la cryptographie des échanges accessible à tous.

⁴ Découlant par exemple du Patriot Act aux États-Unis ou de la loi sur la sécurité quotidienne (LSQ) en France.

⁵ Réglementations dites « *Know Your Customer* » (KYC).

des idées cypherpunks et crypto-anarchistes en prônant la liberté des transactions par le droit à l'anonymat et l'absence de contrôle étatique.

Il apparaît alors que les cryptomonnaies se sont historiquement construites en premier lieu contre l'autorité des États, de leurs gouvernements et des banques centrales, dans une moindre mesure en opposition aux banques commerciales. Nous l'avons vu, ECash, EMS ou encore PayPal sont autant d'« alternatives » aux systèmes de paiements traditionnels pourtant conçues par ou avec l'appui d'entreprises intégrées dans les modèles économiques traditionnels (entreprises de la Silicon Valley ou banques commerciales). Par ailleurs, lorsque Bank of America, Visa, MasterCard, PayPal et Western Unions isolèrent Wikileaks en 2010 en « bloquant » les dons à l'organisation (conformément à ce que la loi exigeait), son fondateur et proche des mouvements cypherpunks¹ Julian Assange regretta publiquement que ces entreprises soient « des instruments de la politique étrangère américaine »². Ce faisant, Julian Assange dénonça comme censeur non pas directement ces entreprises, mais en premier lieu le gouvernement américain. De concert, Jon Matonis, membre fondateur de la Bitcoin Foundation, expliqua alors que Bitcoin était une solution face à l'action d'entreprises qui auraient subi une pression politique. Plus généralement et selon David Golumbia, les cryptomonnaies en général et Bitcoin en particulier semblent s'inscrire dans le phénomène appelé « cyberlibertarisme » dont le principe pourrait être « aucun gouvernement ne doit réguler l'Internet » en corollaire de l'idée selon laquelle la liberté émergera du développement des technologies numériques lui-même³. Le thème de la liberté se comprendrait alors comme une « liberté vis-à-vis des gouvernements » qui auraient un pouvoir uniquement oppressif. Cette conception politique rejoint celle des anarcho-capitalistes comme Murray Rothbard et David Friedman dont les idées ont trouvé des incarnations politiques avec Ronald Reagan aux États-Unis⁴ et Margaret Thatcher au Royaume-Uni. Fondateur du *think tank* libertarien Cato Institute, Murray Rothbard rejette dans son essai *Anatomy of State* (1974) la légitimité démocratique des gouvernements qu'il oppose à la responsabilité politique des institutions privées dont le pouvoir, détenu par le capital ou les marchés, serait responsable vis-à-vis des citoyens. Cette pensée politique s'articule avec la théorie économique monétariste de l'École de Chicago fondée par Milton Friedman, selon laquelle le contrôle de l'offre de

¹ Assange J. (2012), *Cypherpunks: Freedom and the Future of the Internet*, OR Books.

² AFP (2010), « [Assange dénonce Visa, Mastercard et PayPal qui ont bloqué les virements](#) », *Libération*, 14 décembre.

³ Golumbia D. (2016), *op. cit.*.

⁴ Ronald Reagan déclarait dans son premier discours d'investiture en tant que président des États-Unis, le 20 janvier 1981 : « *l'État n'est pas la solution à notre problème ; l'État est le problème* ».

monnaie serait un moyen de contrôle de l'inflation. En concevant une monnaie émise en quantité fixée dès sa naissance selon des règles définies dans le code informatique (contrôle de l'offre monétaire), les concepteurs de Bitcoin semblent s'être approprié la théorie monétariste de l'inflation. Selon David Golumbia, la défiance véhiculée par Bitcoin vis-à-vis des politiques inflationnistes des banques centrales est alimentée par des mouvements de conservateurs aux États-Unis, relayés par l'association John Birch Society (JBS). La JBS considère que l'inflation est une taxe permettant à ceux qui l'organiseraient de déposséder les citoyens par l'augmentation de la quantité de monnaie en circulation¹. L'inflation serait une conséquence des politiques des banques centrales, un outil de captation de valeur par les banques centrales ayant des objectifs cachés autres que la stabilité monétaire, *a contrario* de la définition traditionnelle d'augmentation des prix vue comme une conséquence de ces politiques, elles-mêmes mises en œuvre en réponse à des pressions économiques externes (comme le niveau d'emploi ou l'évolution des prix). Bitcoin et les cryptomonnaies apparaissent ainsi comme les vecteurs d'une idéologie libertarienne promouvant une réduction voire une disparition de l'État afin d'atteindre une société régie par un capitalisme livré aux seules lois d'un marché libre de toute régulation. Ces discours « libertariens » de défiance vis-à-vis des institutions étatiques sont non seulement portés par des activistes qui mettent en garde contre un risque d'intervention des gouvernements dans les échanges en ligne, mais aussi par des soutiens des cryptomonnaies et des blockchains aux intérêts pouvant apparaître éloignés. On trouve parmi eux des « geeks », des investisseurs ou des entrepreneurs. Différentes figures emblématiques du développement de l'industrie numérique occupant des positions d'« intermédiaires » dans le cyberspace se prononcent très favorablement pour Bitcoin et les autres applications qui pourraient être développées sur des technologies similaires, parmi lesquels Eric Schmidt (PDG de Google de 2001 à 2011)² qui encourage le développement de la technologie blockchain comme moyen de développer de nombreux nouveaux usages numériques³ ou encore Elon Musk et Peter Thiel (cofondateurs de PayPal et nommés conseillers par le président des États-Unis Donald Trump)⁴. Elon Musk affirme que la technologie blockchain offre des outils d'architecture informatique pour fluidifier les transactions entre individus, mais aussi que Bitcoin est un moyen d'opérer des transactions illégales, « ce qui n'est pas

¹ The John Birch Society (2009), « What is money? ».

² Priestland D. (2013), « [The libertarian iCapitalists wouldn't have anything to do with the state... would they?](#) », *The Guardian*, 19 juin 2013.

³ « [What does Google's Eric Schmidt think of Bitcoin?](#) », document vidéo, *Youtube*.

⁴ Packer G. (2011), « [No death, no taxes : the libertarian futurism of a Silicon Valley billionaire](#) », *The New Yorker*, 28 novembre.

nécessairement mauvais »¹ selon lui. Peter Thiel, en finançant le projet Ethereum de Vitalik Buterin, apparaît comme un investisseur direct dans la technologie blockchain². Adli Takkal Bataille et Jacques Favier illustrent que les liens assumés entre de grandes entreprises du numérique et les cryptomonnaies sont non seulement idéologiques mais aussi financiers. Les investissements semblent s'être multipliés exponentiellement à mesure que le cours de Bitcoin s'envolait depuis le début des années 2010. À titre d'exemple, la plateforme d'échange de cryptomonnaies Coinbase a levé 600 000 dollars auprès d'entrepreneurs activistes et de fonds californiens en septembre 2012, puis reçu 32 millions de dollars au 31 décembre 2013 dont 25 provenant du fonds de deux anciens de Netscape, Marc Andreessen et Ben Horowitz. Le même fonds associé à d'autres spécialisés dans les cryptomonnaies comme Google Venture ou Bitcoin Opportunity Fund investirent par ailleurs plusieurs millions de dollars dans Ripple, une solution concurrente de Bitcoin destinée aux banques. L'engouement croissant pour Bitcoin, alimenté par la hausse de sa valeur exprimée en devise traditionnelle et par l'essor rapide d'entreprises qui fleurirent dans son écosystème, fit miroiter à de nombreux investisseurs et capital-risqueurs des opportunités profitables qui glissèrent progressivement de la seule « sphère Bitcoin » vers celle de « la blockchain ». En 2014, l'entreprise spécialisée dans des solutions blockchain pour entreprises Chain leva 14 millions de dollars et Blockchain.info en leva 30. Ce transfert d'intérêts financiers de Bitcoin aux blockchains fut relayé par la presse. *The Economist* titra en octobre 2015 « *La machine à confiance, comment la technologie sous-jacente au Bitcoin pourrait transformer la manière dont l'économie fonctionne* »³. Adli Takkal Bataille et Jacques Favier associent le scandale de la plateforme d'échange Silk Road⁴ et les fermetures de comptes bancaires conséquentes au lancement de groupes de travail au sein des banques sur la technologie blockchain. Défenseurs revendiqués du Bitcoin, ces auteurs estiment que les banques opèrent un « revirement opportuniste » et soulignent l'attitude de la « finance institutionnelle » qui retournerait « l'arme [la technologie blockchain] qui la visait [Bitcoin] »⁵. Ils pointent une possible connivence entre les orientations des réglementations en cours d'élaboration autour des technologies blockchain et les institutions financières, en opposition aux idéologies « geeks » et cypherpunks des origines, opposés à toute autorité étatique (voir *supra*).

¹ « [Elon Musk Interview: On Bitcoin and Cryptocurrency](#) », document vidéo, *Youtube*.

² Madelaine N. (2017), « [Ethereum, la blockchain plus sophistiquée que celle de bitcoin](#) », *Les Échos*, 23 janvier.

³ *The Economist* (2015), « The trust machine: the technology behind bitcoin could transform how the economy works », 31 octobre.

⁴ Silk Road organisait un marché noir sur Internet, dont les transactions étaient effectuées en bitcoins.

⁵ *Op. cit.*, p. 220.

Ils dénoncent l'utilisation commerciale par les institutions financières d'une technologie blockchain vue comme un « remède miracle à leur obsolescence informatique », prises qu'elles sont « entre la menace des GAFAM et celles des start-ups de la fintech »¹.

Les principes de cette technologie blockchain sont alors largement médiatisés par les institutions financières elles-mêmes, particulièrement à partir de 2015. Figure emblématique de l'industrie financière, Blythe Masters propose d'« oublier le Bitcoin » et de « se saisir de la blockchain »². Depuis, et en moins de deux ans, la blockchain s'est imposée comme une des premières priorités technologiques à l'agenda de la plupart des institutions financières. Elle se traduit par différentes initiatives de prototypage ou « Proof Of Concept », certaines développées unilatéralement, d'autres en collaboration (de manière *ad hoc* ou *via* des consortia organisant les échanges et retours d'expérience). La blockchain représenterait des opportunités de gains d'efficacité opérationnelle. Les transformations des systèmes d'information avec la blockchain conduiraient à des améliorations de la qualité des échanges (notamment diminution des risques opérationnels, facilité d'accès et de partage de l'information, amélioration des délais de livraison, certifications par construction) ainsi qu'à des transformations des organisations elles-mêmes (redistribution des rôles et des responsabilités des acteurs, transformation des systèmes comptables). Selon le World Economic Forum³, la blockchain pourrait avoir un impact sur des secteurs aussi variés que les paiements, les traitements post-trade, la compliance, les levées de fonds, les montages financiers entre institutions, ou encore l'assurance. Depuis, le nombre d'opportunités de champs d'application semblent se multiplier. Parmi les plus souvent mentionnés on trouve l'énergie, l'Internet des objets (IoT), la gestion des identités, la distribution de contenus numériques, l'administration de patrimoines immobiliers, ou encore la politique et les questions liées à la gouvernance. Cette anticipation « multi-industries » de développements techniques qui permettraient de nouvelles formes d'organisation des transactions, susceptible de « disrupter » l'économie, semble partagée par de nombreux acteurs. Parmi eux figurent des porte-voix de grands groupes industriels ou financiers en coopération, des investisseurs de capital-risque et des entrepreneurs, des sociétés de conseil, de la presse généraliste et spécialisée, des individus qui

¹ *Op. cit.*, p. 229.

² Massa A. (2015), « [Blythe Masters Says Forget Bitcoin, Embrace the Blockchain](#) », *Bloomberg.com*, 6 octobre.

³ World Economic Forum (2016), [The future of financial infrastructure. An ambitious look at how blockchain can reshape financial services.](#)

s'expriment par différents moyens disponibles sur Internet, mais aussi gouvernements et États qui agissent comme utilisateurs¹ ou garants des politiques monétaires et économiques (voir *infra*). Nombre d'entre eux partagent une croyance forte dans les bienfaits d'une « décentralisation » dont la technologie blockchain serait le moyen. Si la volonté de « décentralisation » du pouvoir économique a motivé la création de Bitcoin et des cryptomonnaies (voir *supra*), elle se traduit dans la technologie blockchain dans des formes variées. De nombreuses start-ups développent par exemple des « applications décentralisées »² (DApp) sur des blockchains publiques, comme Ethereum. Elles se revendiquent d'un « Web 3.0 décentralisé » en opposition à des entreprises proposant des services construits sur un modèle de bases de données centralisées, qu'elles critiquent pour leur manque de transparence ou les risques liés à la centralisation des données. Les transactions sont comptabilisées en jetons adossés à la cryptomonnaie de ladite blockchain, par exemple l'ether. Dans les blockchains « de consortium », la technologie peut apparaître comme un moyen de faire converger des processus métier de différents acteurs d'un même secteur d'activités *via* un registre de transactions partagé et « décentralisé », souvent en se passant d'un « tiers de confiance » jusqu'alors nécessaire. La *Monetary Authority of Singapore* (MAS)³ a par exemple travaillé avec différentes institutions financières et représentants de solutions logicielles dans le projet dit « Ubin »⁴ pour évaluer la faisabilité d'une automatisation au moins partielle d'une tenue de registre de cash inter-bancaire en dollar de Singapour (SGD). Ces différentes solutions logicielles⁵, mais aussi Bitcoin, Ethereum ou de nombreuses autres « technologies blockchain » sont développées en *open source*. Les développements *open source* sont vantés pour leur transparence (chacun peut s'assurer qu'aucune fonctionnalité n'est cachée), pour la robustesse qu'ils permettent d'assurer (le code est plus puissant et plus sûr s'il est contrôlable par quiconque), ou encore pour leur ouverture à des initiatives individuelles dans le cadre des blockchains publiques (par exemple, quiconque peut construire une DApp s'appuyant sur le réseau Ethereum)⁶. On observe notamment

¹ Le mouvement populiste « 5 étoiles », première force d'opposition en Italie, propose par exemple des applications de la Blockchain dans les services publics, voir : Reuters (2017), « [RPT-Anti-establishment wave to help push blockchain into real world in 2017](#) », Reuters, 11 janvier 2017.

² Appelées DApp, abréviation de « *Decentralized APPLication* », ces applications sont construites à l'aide de *smart contracts* qui font l'interface entre la base de données décentralisée (souvent désignée « blockchain ») et l'application web de l'utilisateur.

³ Banque centrale de Singapour.

⁴ Détails du projet et rapports disponibles sur la page de la MAS.

⁵ Corda, Hyperledger Fabric et Quorum.

⁶ L'*open source* est notamment défendu par Eric Raymond, libertarien actif et revendiqué. Dans le monde des logiciels libres, il s'est construit en opposition au *free software* qui est lui défendu par la

cette approche dans le développement des protocoles sur lesquels des applications ou distributions privées (à code ouvert ou pas) sont construites.

Si les dirigeants des grandes institutions financières publiques nationales ou supranationales mettent régulièrement en garde contre l'utilisation des cryptomonnaies dans leur état actuel, ils sont souvent ouverts voire bienveillants vis-à-vis des possibles applications de la technologie blockchain. Jean-Claude Trichet s'est déclaré méfiant vis-à-vis de « l'instrument spéculatif » Bitcoin¹ : le directeur de la Banque de France de 1993 à 2003 puis gouverneur de la Banque centrale européenne (BCE) de 2003 à 2009 expliquait alors que les cryptomonnaies ne pourraient pas se substituer aux monnaies gouvernées par les États en raison de l'instabilité de leur cours. En revanche, Jean-Claude Trichet qualifie la blockchain d'« invention géniale, parce qu'elle repose sur une décentralisation complète de l'enregistrement des transactions », investie par les banques commerciales pour préserver le service à leurs clients en abaissant leurs coûts. L'enthousiasme de l'ancien président de la BCE tranche avec les discours de son actuel président, Mario Draghi, plus réservé sur l'utilisation de la blockchain². Dans une allocution officielle, il estime que le développement rapide de la technologie induit de la part de la BCE une attitude de « surveillance permanente » et d'« estimation des risques » portant sur la sécurité et l'efficacité des systèmes de paiements et des infrastructures de marchés – en particulier les activités de règlement et de compensation sur les marchés de capitaux. Mario Draghi pointe notamment le risque que pourrait représenter la mise en œuvre de blockchains par différents États membres de l'Eurogroupe. Le président de la BCE a par exemple fermement condamné toute initiative de mise en œuvre par un État membre d'une cryptomonnaie nationale en rappelant que « la seule monnaie de l'Eurozone est l'Euro »³. La prudence de la BCE vis-à-vis de possibles innovations qui pourraient naître d'applications de la technologie blockchain est en premier lieu dirigée vers les cryptomonnaies existantes en général et vers Bitcoin en particulier.

Free Software Foundation de Richard Stallman. Alors que ce dernier met en avant les mérites éthiques et philosophiques des logiciels libres, Eric Raymond rejette cette rhétorique qu'il juge normative et préfère souligner la qualité des logiciels à code source ouvert d'un point de vue purement technique, utilitaire et économique. Eric Raymond pense par-là convaincre plus efficacement le grand public ainsi que les entreprises d'adhérer aux principes des logiciels libres, et en conséquence contribuer aux liens entre développeurs et investisseurs.

¹ Damien Leloup (2016), « [Jean-Claude Trichet à propos du bitcoin : "La blockchain est une invention géniale"](#) », *Lemonde.fr*, 2 octobre.

² Draghi M. (2017), *Hearing of the Committee on Economic and Monetary Affairs of the European Parliament*, 29 mai.

³ Reuters Staff (2017), « [ECB's Draghi rejects Estonia's virtual currency idea](#) », *Reuters*, 7 septembre.

Suite à une déclaration dans laquelle Mario Draghi affirmait que la BCE n'a « pas de pouvoir » pour réguler Bitcoin¹, largement relayée par de nombreux sites soutenant les cryptomonnaies, le gouverneur de la BCE a précisé que Bitcoin n'était pas assez mature pour attirer la considération de la BCE. Si Mario Draghi n'indique pas d'intention claire pour intervenir sur les cryptomonnaies ou les utilisations de blockchains, il apparaît qu'une réglementation spécifique par la BCE serait envisageable. Mario Draghi réaffirme par là le mandat de la BCE, seule institution responsable de l'organisation des échanges monétaires au sein de la zone euro : les applications des blockchains sont susceptibles d'être encadrées par la BCE si et seulement si elles impactent l'ordre monétaire dont la BCE est garante. Christine Lagarde, directrice du FMI depuis 2011, rappelle elle aussi la centralité des banques centrales dans une période marquée par l'émergence de nombreuses innovations financières, voyant dans le FMI une « plateforme idéale » pour les discussions autour de ces nouvelles technologies². Tout en pointant certaines limites majeures des cryptomonnaies à ce jour, la directrice du FMI estime que ces limites techniques pourraient être dépassées et qu'il ne serait aujourd'hui « pas sage » d'ignorer les cryptomonnaies. Christine Lagarde estime que les cryptomonnaies ne représentent pas de menace pour l'ordre existant des devises traditionnelles et des banques centrales, mais qu'elles devraient au contraire être transformées en opportunités par les banques centrales et les États. Selon Christine Lagarde, la meilleure réponse des banquiers centraux serait de continuer à mettre en œuvre des « politiques monétaires efficaces » en étant ouverts aux « idées fraîches et nouvelles demandes » à mesure que l'économie évolue. En ce sens et d'une part, les cryptomonnaies pourraient représenter un instrument monétaire adossé à une ou des monnaies traditionnelles au travers desquelles les politiques monétaires pourraient continuer de s'exercer ; d'autre part, les banquiers centraux pourraient être amenés à soutenir l'émergence de nouveaux services de paiement issus de l'utilisation des cryptomonnaies.

Dans les processus d'innovations autour de la technologie blockchain, s'engagent des acteurs nombreux et variés. Une représentation séminale semble être partagée par les utilisateurs de cryptomonnaies, par les entrepreneurs qui innovent et développent la technologie blockchain comme par les dirigeants des institutions mettant en œuvre les politiques monétaires : la « décentralisation » et la création de

¹ O'Leary R. R. (2017), « [Mario Draghi: European Central Bank Has 'No Power' to Regulate Bitcoin](#) », *CoinDesk.com*, 26 septembre.

² Lagarde C. (2017), « [Central Banking and Fintech – A Brave New World?](#) », *International Monetary Fund*, 29 septembre.

réseaux *ad hoc* hors des canaux de distribution traditionnels. Les blockchains seraient les supports d'infrastructures en réseaux permettant à leurs membres, personnes physiques ou morales, d'échanger de pair-à-pair sans intermédiation par une autorité centrale. Les applications réelles ou projetées de la technologie blockchain laissent imaginer de nouveaux réseaux ou une restructuration de réseaux existants. On assiste à des tentatives d'autonomisation d'entités jusqu'alors reliées par des dispositifs techniques ou institutionnels qui sont remis en question. Le service proposé par Ethereum offre par exemple la possibilité de créer des organisations décentralisées, les DAOs / DACs¹, supposées fonctionner « sans intervention humaine ». Dans le modèle proposé par Ethereum, les mouvements de capitaux seraient régis par les stratégies des agents reproduites et automatisées dans le code informatique. Ces dispositifs, à défaut d'être régulés par les États, pourraient l'être par la « loi du marché ». Cette perspective, et plus généralement les blockchains, soulèvent la question politique du rôle des États dans l'encadrement des mouvements de capitaux et les nouvelles formes que les logiques d'accumulation du capital pourraient prendre. Les blockchains permettraient en effet et non seulement de consolider des réseaux d'entités aux intérêts divergents qui pourraient collaborer par la mise en place de processus partagés (blockchains entre institutions financières ou particuliers, par exemple), mais aussi de fédérer des initiatives d'acteurs aux motivations *a priori* éloignées : développeurs, libertariens, militants d'une « décentralisation » de l'Internet, investisseurs en capital-risque, banques centrales, start-ups, développeurs. Il apparaît ainsi que, si elles ne sont ni de simples curiosités techniques ni des instruments économiques révolutionnaires, les blockchains sont susceptibles de cristalliser des débats idéologiques et politiques profonds et anciens.

Remerciements pour leur lecture attentive, leurs commentaires et les discussions que l'écriture de ces lignes a fait naître, à l'ensemble du groupe de travail et tout particulièrement à Joëlle Toledano, Lionel Janin, Jacques Favier et Xavier Simonin, ainsi que Fabian Muniesa (MINES ParisTech) et Kevin Mellet (Orange Labs).

¹ Acronymes de « Decentralized Autonomous Organizations » et « Decentralized Autonomous Corporations ». Vitalik Buterin les décrit comme des entités qui vivent indépendamment sur internet, disposant d'un capital interne et d'une propriété propre.



LES ENJEUX JURIDIQUES DE LA BLOCKCHAIN

RAPPORT DU SOUS-GROUPE JURIDIQUE

Le groupe de travail de France Stratégie sur les blockchains a constitué un sous-groupe juridique pour examiner le cadre légal et réglementaire dans lequel les cas d'usage de la blockchain s'inscrivaient et proposer des axes d'amélioration. Les membres de ce groupe ont invité des acteurs spécialisés du secteur à participer à leurs travaux¹. Ce document constitue le rapport établi par ce sous-groupe.

La technologie dite « blockchain » et ses mécanismes de consensus permettant de garantir l'unicité d'inscriptions et la transférabilité d'unités de comptes numériques font naître de nouvelles problématiques juridiques que le droit français n'appréhende pas encore parfaitement. Il n'est pas isolé ; en dehors d'initiatives sporadiques, l'état du droit de la blockchain est encore balbutiant. C'est une opportunité pour la France de se positionner à l'avant-garde dans un domaine à l'importance stratégique.

Sans revenir en détail sur les caractéristiques techniques de la technologie, ce rapport s'attachera à analyser ses différents cas d'usage au regard des enjeux juridiques qu'ils posent. Il porte un double objectif de diagnostic et de proposition.

Dans un premier temps, il établit un état des lieux des problématiques juridiques posées par la blockchain aux acteurs qui souhaitent s'en saisir et développer des activités autour de cette technologie, qu'elles soient commerciales, industrielles, sans but lucratif ou d'intérêt général. Dans ce contexte, les participants au rapport ont identifié les points de tension, les problématiques qui seraient de nature à freiner ou bloquer les expérimentations ou projets en cours.

Dans un second temps, des propositions concrètes permettant d'amoindrir ou de supprimer les points de tension identifiés ont été formulées pour les principaux cas d'usage, en miroir de ces problématiques. Elles l'ont été en gardant à l'esprit la

¹ La rédaction de ce rapport a été achevée en février 2018. La liste complète des contributeurs figure en fin d'annexe p. 124.

nature expérimentale de ces technologies et le besoin de définir des cadres appropriés qui pourront s'adapter aux futures évolutions de la technologie.

Parmi celles-ci, trois propositions nous semblent devoir être mises particulièrement en avant car elles répondent à des impératifs immédiats vécus par les acteurs du secteur.

- **Question de la preuve** : le groupe de travail pointe l'insécurité naissant de l'absence de régime de preuve spécial relatif à l'inscription sur blockchain et recommande une adaptation du droit existant pour permettre la prise en compte, sous certaines conditions détaillées dans la fiche correspondante, d'une inscription sur blockchain comme preuve. À court terme, il est possible d'adopter une réforme visant à renforcer, dans le code civil, la force probante des informations figurant sur une blockchain selon des modalités techniques à préciser. Dans une perspective de plus long terme, il faudra engager une réflexion devant aboutir à la révision du règlement eIDAS afin de reconnaître pleinement la fiabilité de la signature électronique et de l'horodatage sur la blockchain sans intervention d'un tiers certificateur.
- **Fiscalité**. Le groupe de travail a également identifié la question fiscale, et plus particulièrement l'imprécision qui pèse aujourd'hui sur le traitement fiscal des opérations, comme étant un frein important au développement des activités relatives à la blockchain sur le territoire français. *A contrario*, une politique fiscale claire et adaptée à cette nouvelle classe d'actifs serait de nature à attirer des acteurs sérieux sur le territoire. La recommandation du groupe de travail est de clarifier, par la loi, le régime fiscal des cybermonnaies. En pratique, ceci suppose de clarifier fiscalement le régime des opérations d'achat, de vente mais aussi les échanges et autres utilisations de cybermonnaies et *tokens*. Il est également recommandé de clarifier l'exonération des échanges d'actifs numériques de la taxe sur la valeur ajoutée.
- **Ouverture de compte bancaire**. Le groupe de travail a enfin constaté que de nombreux acteurs étaient confrontés à une problématique liée à l'ouverture et au fonctionnement de leurs comptes bancaires. Les contraintes imposées aux établissements de crédit en matière de lutte contre le blanchiment et le financement du terrorisme ne tiennent pas compte des particularités des cybermonnaies. Ceci est de nature à constituer un obstacle à l'ouverture et au fonctionnement de tels comptes voire à provoquer leur fermeture, quand bien même les transactions réalisées avec ces actifs ne seraient pas suspectes. Le groupe de travail recommande d'imposer aux entreprises gérant des plateformes d'échange des obligations de vérification d'identité et d'origine des fonds (KYC et AML) ainsi que la communication aux titulaires de comptes de toutes les informations leur permettant de satisfaire les exigences réglementaires

applicables aux établissements de crédit. Ceci permettra aux établissements bancaires de satisfaire leurs propres obligations en la matière afin de ne pas bloquer le fonctionnement de ces comptes.

Le rapport est composé de cinq fiches de synthèse correspondant aux cas d'usage identifiés de la technologie d'une part, et aux branches du droit concernées d'autre part. Chaque fiche est appréhendable séparément mais certaines problématiques spécifiques se répondent naturellement.

Bonne lecture.

Au nom du sous-groupe juridique,
Simon Polrot

Les cinq fiches

Fiche 1 – Analyse juridique des tokens ou jetons

Fiche 2 – *Smart contracts* et droit des contrats

Fiche 3 – Preuve et signature numérique

Fiche 4 – Fiscalité

Fiche 5 – Enjeux de conformité et droit au compte



Fiche 1

Analyse juridique des *tokens* ou jetons

Responsable de rédaction

Hélène Lefebvre, avocate associée, Fieldfisher LLP

Le jeton ou « token » est un objet numérique sur une blockchain, et peut résulter de deux processus de création distincts :

- soit il est créé directement par le code-source du protocole de la blockchain et généré par une activité de minage. On parle alors aussi de cybermonnaies pour les principaux réseaux (bitcoin, ether, etc.) ;
- soit il est créé par un « *smart contract* », sur une chaîne préexistante, qui détermine notamment leur nombre initial et leurs modalités d'émission.

Les tokens sont initialement proposés dans le cadre des Initial Coin Offering (ICO) ou distribués directement, avec ou sans contrepartie¹. Ils sont ensuite le plus souvent échangés entre pairs ou sur des places de marché ou plateformes leur permettant ainsi d'acquérir une valeur de marché, bien que celle-ci soit généralement volatile.

Appréhender la nature juridique des tokens

Caractéristiques multiples

Les tokens sont librement programmés lors de leur création. Chaque token étant programmé pour une utilisation déterminée, leurs caractéristiques peuvent être multiples (voir leur typologie page suivante). Ainsi, qualifier juridiquement le token ne peut reposer sur le simple fait qu'un instrument est qualifié génériquement de « token » ; il convient de prendre en compte leurs caractéristiques précises.

¹ La question du traitement juridique des ICO fait l'objet d'une consultation publique de l'Autorité des marchés financiers concomitante à la réalisation de ce rapport et ne sera par conséquent pas examinée en détail.

Utilisation double

En outre, ces instruments pourront être programmés pour une utilisation donnée (ses caractéristiques de départ) et être, en cours de cycle, utilisés d'une manière différente par les détenteurs du token. En tout état de cause, la plupart des tokens peuvent être utilisés comme « cybermonnaie », c'est-à-dire une unité de compte numérique à valeur d'échange. Un même instrument pourra donc, par exemple, avoir été créé pour représenter un droit de vote dans un projet et être également utilisé comme instrument d'échange.

Typologie des tokens

S'il est impossible de dresser une liste exhaustive des cas d'usage, les principaux tokens que l'on peut voir sur le marché à la date de ce rapport correspondent aux caractéristiques suivantes :

- *tokens applicatifs* : ces tokens sont utilisés dans une application décentralisée déterminée et permettent d'accéder à un service donné, comme les « RLC », émis par IEx.ec et permettant d'accéder à de la puissance de calcul ;
- *tokens de réputation* : ces tokens sont utilisés aux fins d'apprécier la fiabilité d'un utilisateur de la technologie blockchain. Dans ce contexte, le nombre de tokens attribués à l'utilisateur peut refléter son niveau de fiabilité : on pourra citer les tokens « REP » émis par Augur ;
- *tokens donnant droit à un revenu ou un dividende* : le token est créé en lien avec un projet particulier et donne le droit de recueillir des revenus liés au projet à des intervalles prédéfinis. Les tokens « The DAO » offraient un droit à percevoir des revenus issus des projets financés ;
- *tokens de vote* : ces tokens représentent un nombre de voix prédéterminé et pourront être utilisés dans un *smart contract* de vote. Les tokens « MKR » de « maker DAO » donnent ainsi un droit de vote à leurs détenteurs ;
- *tokens représentant des points de fidélité* : le token est attribué à un client à chaque utilisation d'un service déterminé, ce token, à l'image de celui émis par « Plutus », pourra ensuite être utilisé en paiement ou selon d'autres modalités ;
- *tokens représentant une valeur spécifique* : ces tokens peuvent correspondre à une valeur déterminée exprimée par exemple en devise. À titre d'illustration, un token ETH-EURO, par exemple, pourrait être programmé de manière à ce que sa valeur soit toujours égale à un euro ;

- *tokens de preuve* : ces tokens peuvent apporter la preuve de la propriété, de la possession ou du transfert d'un actif non virtuel. Le token est alors lié audit actif et le transfert du token matérialise le transfert de propriété de l'actif non virtuel.

En synthèse, il est cependant possible d'établir plusieurs catégories de tokens selon leur utilisation.

- **Tokens d'investissement.** Cette catégorie comprend les cas où des instruments financiers traditionnels, tels que des actions ou des parts d'une société voire des parts ou actions d'un fonds d'investissement, sont représentés par un token. Ces tokens peuvent donc donner des droits similaires à ceux existants pour des instruments financiers classiques, mais avec la particularité d'exister en tant que token sur une blockchain. Ces tokens d'investissement devraient logiquement tomber dans le champ d'application des réglementations existantes en matière d'instruments financiers ; toutefois, il serait pertinent d'examiner une possible adaptation de ces réglementations pour prendre en compte les améliorations technologiques des tokens concernées, notamment l'influence en termes de transparence.
- **Tokens « biens de consommation ».** Cette catégorie est composée des tokens représentant l'accès à des biens ou services sous forme d'un actif digital consommable, tels qu'une licence d'utilisation ou des droits d'accès à une plateforme digitale. L'objectif de ces tokens est d'être utilisés, « consommés ». Ces tokens de consommation ne sont pas *a priori* des instruments financiers.
- **Tokens « monétaires ».** Il s'agit de jetons qui sont utilisés comme valeur d'échange (« monnaie ») par une communauté définie pour accéder à des biens ou des services au sein de cette communauté.
- **Autres tokens.** Cette catégorie recouvre les tokens qui ne sont ni des tokens d'investissement ni des tokens « biens de consommation ». Les tokens sont d'emploi trop récent pour qu'on puisse présager des nombreuses manières dont ils seront effectivement utilisés dans le cadre du fonctionnement d'un réseau basé sur des tokens. Il est donc difficile de concevoir les limites précises entre les différentes catégories de tokens, et d'anticiper les prescriptions légales nécessaires pour encadrer ces tokens.

Possibles qualifications juridiques des tokens

Qualification générale

D'une manière générale, il est possible de voir dans un token un droit ou *bien incorporel*. Le token peut aussi se rattacher à un régime juridique déjà existant.

Monnaie électronique

La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une *créance sur l'émetteur*, qui est émise contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique¹. Certains tokens peuvent être qualifiés comme de la monnaie électronique même si tous les tokens monétaires ne répondent pas à la qualification de monnaie électronique.

Services de paiement

Les *tokens* (y compris les cybermonnaies) n'entrent pas *a priori* dans la catégorie des services de paiement (au sens des directives européennes DSP I et DSP II).

Titres financiers

Certains tokens, notamment les tokens donnant droit à des revenus et/ou des droits de gouvernance dans une structure (une société ou toute autre forme d'organisation) pourraient s'apparenter à des instruments financiers.

Les instruments financiers, qui comprennent les valeurs mobilières, ont pour caractéristiques d'être (i) émis, notamment, par une personne morale, (ii) inscrits en compte ou susceptibles de l'être, (iii) cette dernière inscription s'effectuant au profit du propriétaire des titres, (iv) négociables et (v) dématérialisés. Pour autant, la définition de valeur mobilière au sens de la directive MIF2 est plus large que la seule définition française et pourrait conduire certains tokens à être caractérisés comme tel. En effet, la définition de valeur mobilière dans la directive MIF2 peut être interprétée très largement.

À cet égard, il convient de noter que la SEC aux États-Unis s'appuie sur la jurisprudence *Howey* de la Cour suprême pour caractériser un instrument ou un droit de « *Security* ». Or l'un des critères clés pour distinguer un « *Security* » (lequel est en droit américain défini très largement) d'un autre bien ou droit réside notamment dans la contrepartie financière accordée aux porteurs de tokens, sous forme de dividendes ou de revenus ou promesse de revenus, autrement dit l'existence d'un rendement financier (critère d'ailleurs retenu pour caractériser en France un « bien atypique »).

Le même besoin de clarification existe pour certains tokens et leur qualification en créance ou titre de créance obligataire, notamment suite à l'arrêt de la Cour de cassation du 23 novembre 2017.

¹ Article L. 315-1 du Code monétaire et financier.

Les titres financiers, qui comprennent les valeurs mobilières¹, sont, en droit français, une catégorie d'instruments financiers, et ont pour caractéristiques d'être (i) émis, notamment, par une personne morale, (ii) inscrits en compte ou susceptibles de l'être², (iii) cette dernière inscription s'effectuant au profit du propriétaire des titres, (iv) négociables et (v) dématérialisés³.

Conclusion

Une analyse au cas par cas des caractéristiques du token est nécessaire afin de qualifier juridiquement ce dernier et d'analyser s'il peut ou non être assimilé à une catégorie juridique déjà existante. Nous pensons que les tokens ne doivent pas déroger à l'application du droit commun et/ou aux droits spéciaux, le cas échéant applicable. Ce qu'il convient d'éviter, c'est d'imposer un cadre juridique entièrement nouveau à des tokens qui sont appréhendables par le droit existant. Nous pensons au contraire que la plupart des catégories juridiques existantes permettent de caractériser juridiquement de très nombreux tokens. Cette analyse préalable est d'autant plus nécessaire que, selon la qualification juridique, la vente du token répondra à tel ou tel régime juridique. Ainsi, un token qualifié de valeur mobilière devra répondre à la réglementation sur l'offre au public de titres, alors qu'un token qualifié de vente d'un service répondra plutôt au droit de la vente à distance.

Si la question de la vente de tokens n'est pas couverte spécifiquement par ce rapport car elle fait l'objet concomitamment d'une initiative de place de la part de l'autorité des marchés financiers, il convient de noter que les conclusions de cette consultation seront déterminantes pour la détermination du statut des tokens.

Recommandations

- 1) *Clarification du cadre juridique des tokens.* Compte tenu du fort développement de l'industrie, il semble nécessaire de préciser le cadre juridique des tokens. Cette clarification devra cependant prendre en compte les qualités intrinsèques du token et son utilisation effective. Une tentative de réglementation par une approche globale, qui aurait pour objectif de faire entrer tous les tokens dans un champ restreint sans prendre en compte les caractéristiques de chacun d'entre eux serait inadaptée.

De façon pragmatique, le groupe de travail conseille le lancement d'une consultation avec les acteurs de la place afin d'identifier les catégories juridiques dans lesquelles

¹ Au sens de l'article L. 228-1 du Code de commerce.

² Articles L. 211-3 à L. 211-13 du Code monétaire et financier.

³ Ils se transmettent par virement de compte à compte, article L. 211-16 du Code monétaire et financier.

les tokens pourraient entrer en fonction de leurs caractéristiques spécifiques. Compte tenu des modalités de création d'un token, certains d'entre eux devraient appartenir à plusieurs catégories.

Une fois ces catégories définies et expliquées, les émetteurs de tokens seraient responsables de la catégorisation de ceux-ci et de l'application de la réglementation y afférente. Dans un souci de prévisibilité juridique, il serait également souhaitable de mettre en place une procédure d'examen préalable par un certain nombre d'institutions publiques des caractéristiques d'un token afin de faire valider *a priori* la catégorisation juridique de ceux-ci.

2) *Cadre réglementaire existant et extension possible.* Les plateformes effectuant pour le compte de leurs clients des opérations d'achat ou de vente de cybermonnaies contre une monnaie ayant cours légal sont soumises à agrément car elles effectuent une prestation de service de paiement (encaissement de fonds pour le compte de tiers, par exemple). Eu égard au développement rapide des tokens et au fait que ceux-ci peuvent faire l'objet d'échanges sans qu'une devise ayant cours légal ne soit impliquée, ce cadre réglementaire pourrait être étendu aux plateformes d'échange ne proposant que des échanges de cybermonnaies.

Quelle que soit l'approche de réglementation choisie, il conviendra d'analyser les textes déjà applicables, afin d'éviter de soumettre un token particulier à plusieurs réglementations et de prévoir, en cas de conflit entre textes applicables, quelle réglementation devra primer.



Fiche 2

Smart contracts et droit des contrats

Responsables de rédaction
Anne-Hélène Le Trocquer, avocat associé, De Gaulle Fleurance et Associés
et Xavier Lavayssière, fondateur, ECAN

Définition

Un *smart contract*, ou contrat intelligent, est un **programme informatique exécuté de façon autonome** par un réseau reposant sur les technologies blockchain. L'expression est une référence au concept plus large de protocole informatique de contractualisation formalisé par Nick Szabo dans les années 1990¹.

Concept et implémentations

Un *smart contract* est habituellement rédigé dans un langage informatique de haut niveau², lisible par tout développeur. Le code est ensuite compilé (transformé) dans un langage machine puis déployé sur un réseau blockchain.

Le *smart contract* est alors accessible au travers d'un identifiant et il est possible d'interagir avec lui par l'intermédiaire de transactions blockchain avec un client logiciel. L'éditeur du *smart contract* ne maîtrise alors ni l'exécution ni l'interface finale avec laquelle l'utilisateur interagit avec le *smart contract*. Déployé sur un réseau blockchain public, ces programmes peuvent gérer de façon native des fonds au travers d'une cryptomonnaie ou d'un jeton.

Propriétés

- *Autonome* : une fois déployé, il n'est pas possible de modifier ou d'empêcher l'exécution du *smart contract* sauf par des procédures prévues au préalable dans son code.

¹ Szabo, N. (1996). Smart contracts: building blocks for digital markets.

² Un langage de programmation de haut niveau est un langage proche des langages naturels, par opposition aux langages de bas niveau plus proches du fonctionnement des machines. Les langages de Smart Contracts sont inspirés de langages de programmation usuels: Solidity et Viper sur Ethereum, Go sur Hyperledger sous l'appellation Chaincode,...

- *financier* : il est possible via le *smart contract* de gérer des fonds, recevoir des paiements et de générer un versement en tokens.
- *traçable* : chaque exécution est tracée par une transaction enregistrée dans la blockchain. De plus, chaque interaction avec le *smart contract* est identifiée à une adresse individuelle, et donc un individu ou un autre *smart contract*.
- *déterministe* : le programme s'exécute selon les procédures décrites par le code sans aléa, sous réserve d'erreur logicielle.

Smart contract et droit français

Le *smart contract* est en pratique : soit une modalité d'exécution d'une relation contractuelle ; soit lui-même le support du contrat. Dans le premier cas, la principale caractéristique qui le distingue d'un logiciel classique est l'autonomie de son exécution (voir infra).

Dans le deuxième cas, que l'on voit notamment avec certaines *Initial Coin Offerings* (ICO)¹, rien ne s'oppose en principe à la reconnaissance de sa valeur légale puisqu'en droit français, le contrat naît de l'accord de volonté des parties² et son support peut être oral, écrit ou numérique (voir infra).

Smart contract comme modalité d'exécution d'une relation contractuelle préexistante

Lorsqu'il s'agit d'un acte d'exécution automatique d'un contrat préexistant, deux approches peuvent être proposées pour en préciser la nature juridique.

Dans une première hypothèse, quand aucun accord de volonté supplémentaire n'est nécessaire pour déclencher la prestation (remboursement dans le cadre d'une assurance retard, par exemple) c'est un acte d'exécution d'une obligation d'un contrat préexistant et à ce titre aucun régime spécifique n'est à créer.

Dans une seconde hypothèse, si une volonté est nécessaire pour mettre en œuvre le *smart contract*, il peut alors être considéré comme un contrat à part entière. Le contrat initial peut alors s'envisager comme un contrat cadre et le smart-contract comme un contrat d'application en précisant les modalités d'exécution³.

¹ Dans le cas où l'ICO consiste en la vente automatique d'un token au travers d'un Smart Contract. C'est ainsi le cas de *The DAO*, en mai 2016, et des projets français iExec et Beyond the Void. Les projets plus récents tendent toutefois à faire signer un contrat au préalable, l'échange sur la blockchain n'étant alors qu'une modalité d'exécution.

² Article 1101 du code civil.

³ « Le contrat cadre est un accord par lequel les parties conviennent des caractéristiques générales de leurs relations contractuelles futures. Des contrats d'application en précisent les modalités d'exécution » Article 1111 du code civil.

Smart contract en tant que support unique du contrat

Dans les cas où le *smart contract* est le seul support d'un contrat, il semble nécessaire que le consentement de l'ensemble des parties soit clairement recueilli et qu'il soit exempt de vice pour que ce contrat numérique soit valable (art. 1127 et suivants du Code civil).

Il conviendra notamment ici de vérifier que les conditions posées par l'article 1127-1 du Code civil (applicable à « quiconque propose à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services, **met à disposition les stipulations contractuelles applicables** d'une manière qui permette leur conservation et leur reproduction ») soient appliquées, en particulier celle relative à la communication des étapes à suivre pour conclure ledit contrat par voie électronique, ainsi que des conditions générales et/ou particulières d'utilisation qui, avec le contrat principal, forment l'ensemble contractuel applicable entre les parties.

Quant à la valeur de l'écrit sous forme de programme, il convient de distinguer les situations. En matière civile, dans le cas d'une contestation entre un professionnel et un particulier dont la valeur n'excède pas 1 500 euros, le contrat peut être prouvé par tout moyen, de même en matière commerciale pour les actes de commerce quel que soit le montant de la transaction (L. 110-3 du Code de commerce). Dans les autres cas, si le programme pourra être considéré comme un écrit en tant que « suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support » (article 1365 du Code civil), il faudra considérer les éléments d'identification et de conservation du programme (voir la fiche « Preuve et signature numérique »).

Conséquences de l'exécution autonome

Le *smart contract* est un programme qui permet de garantir l'exécution d'engagements pris sans intervention humaine directe. Par principe, le programme n'est pas modifiable une fois déployé sur la blockchain. Cette immutabilité est donc susceptible de créer des situations de fait difficiles à résoudre juridiquement. Les procédures de modification et situations doivent donc être anticipées dans le code, entre les parties et dans le cadre juridique :

- la modification avec l'accord des deux parties et la rétractation d'une des parties ;
- la mauvaise exécution issue d'une erreur de manipulation ou tentative frauduleuse ;
- les bugs ou mauvais fonctionnement du programme. Des questions de responsabilité extra contractuelle peuvent se poser dans ce cas entre les parties

et vis-à-vis des prestataires et éditeurs de solutions majoritairement *open source*¹.

- les effets de l'annulation du contrat original, de l'intervention du juge ou éventuellement d'arbitres, de l'ouverture d'une procédure collective...

Juridiquement, il faut constater que l'automaticité du processus empêche le jeu normal des dispositions sur l'inexécution du contrat des articles 1217 et suivants du Code civil. C'est donc en effet par des mesures correctrices que les remèdes aux difficultés d'exécution ou aux vices affectant le *smart contract*, voire son contrat cadre, doivent être pensés.

Recommandations

- 1) Préciser explicitement, potentiellement par la loi, les conditions dans lesquelles un *smart contract* pourrait avoir une valeur de contrat formel, de façon similaire au travail accompli en matière de contrats sous forme électronique. Ce travail s'effectuera en lien avec les recommandations proposées en matière de preuve.
- 2) Développer un référentiel de bonnes pratiques pour le développement de *smart contract* sécurisés, notamment quand ils sont amenés à manipuler des fonds.

¹ Les programmes *open source* sont des programmes dont le code source est publié de façon publique et comportant généralement une clause limitative de responsabilité des auteurs. Les plus connues ont la GNU Public Licence, MIT License et BSD License.



Fiche 3

Preuve et signature numérique

Responsable de rédaction
Florence G'sell, professeur agrégé de droit privé

Les algorithmes utilisés par les chaînes de blocs participent à l'état de l'art des meilleures solutions cryptographiques connues. Les caractéristiques techniques de ces chaînes permettent de faire en sorte que les informations inscrites sur les blockchains soient accessibles sans risque d'interruption et ne soient ni effaçables, ni modifiables ni répudiables. Elles sont publiquement visibles et auditable par tout participant au réseau. Tel est l'apport de la technologie blockchain dont le droit de la preuve doit tenir compte.

1. Enjeux

Les questions de la preuve électronique et de la signature numérique constituent des enjeux majeurs pour le déploiement de la technologie blockchain. De nombreux développements en cours portent, en effet, sur des applications permettant d'effectuer diverses transactions ou de certifier la réalisation de certains événements (livraison de marchandises, création d'une œuvre originale, etc.). Il convient donc de faire en sorte que ce qui se trouve sur la blockchain puisse disposer d'une portée probatoire avérée, faute de quoi l'investissement dans cette technologie se révélera dépourvu d'intérêt dans la mesure où il faudra recourir aux tiers de confiance traditionnels.

Le droit français étant fondé sur un système de preuve légale, ce sont les textes législatifs et réglementaires qui prévoient la portée juridique des différents éléments de preuve soumis au juge. Dès lors que la blockchain ne peut être assimilée à l'un des moyens de preuve actuellement reconnus juridiquement et qu'aucun texte n'en prévoit la portée juridique, l'incertitude prédomine. Il est, en effet, impossible d'anticiper ce que le juge français pourrait décider face à un élément de preuve émanant d'une blockchain. Cette situation est génératrice d'une insécurité juridique de nature à freiner l'attrait de cette technologie pour les opérateurs.

Il convient donc de s'assurer que la preuve de type « blockchain » se voit conférer une portée juridique reflétant la fiabilité revendiquée par la technologie.

2. État des lieux concernant la preuve sur la blockchain

Les questions probatoires ne se posent pas dans les mêmes termes selon que la blockchain est privée ou publique.

2.1. La preuve sur une blockchain privée

Sur une blockchain privée et permissionnée, il suffit que le(s) gestionnaire(s) du réseau propose(nt) aux utilisateurs autorisés à y accéder une convention de preuve prévoyant que lesdits utilisateurs acceptent de considérer comme recevables en cas de litige des éléments techniques issus de la blockchain.

En cas de litige, le juge statuera sur la validité de la convention de preuve judiciaire et sur sa portée. Cela signifie qu'il suivra en principe les stipulations de la convention de preuve mais pourra, le cas échéant, être amené à apprécier lui-même la portée des éléments de preuve soumis par les parties. La Cour de cassation n'a pas accepté, conformément à l'article 1356 du Code civil, qu'une convention de preuve prévoie des présomptions irréfragables, qui ne peuvent être renversées, au bénéfice de l'une des parties (Cass. com. 6 décembre 2017, n°1517, 16-19615).

Bien que les difficultés probatoires puissent être réglées, sur des blockchains privées, par des conventions de preuve suffisamment précises et licites (pas de clause abusive, par exemple), cette situation n'est pas entièrement satisfaisante. Il se peut fort bien, par exemple, que l'on soit confronté en pratique à des conventions de preuve insuffisamment rédigées et que cela génère du contentieux. Il serait certainement préférable que le droit commun règle une fois pour toutes la question de la preuve sur la blockchain.

2.2. La preuve sur une blockchain publique

Sur une blockchain publique et entièrement décentralisée, la conclusion de conventions de preuve n'est pas envisageable. La preuve sur la blockchain pose alors de réelles difficultés.

Il convient d'aborder en premier lieu la preuve des actes juridiques, qui sont en général des actes sous seing privé librement conclus entre deux personnes privées (2.2.1), avant de dire quelques mots du cas particulier des actes authentiques (2.2.2.), puis d'évoquer le cas des simples faits juridiques (2.2.3.).

2.2.1. La preuve d'un acte sous seing privé sur une blockchain

La preuve des actes sous seing privé conclus sur une blockchain obéit à des règles générales figurant dans le Code civil (a) et pose la question plus spécifique de la signature électronique (b) ainsi que celle de l'horodatage (c).

a) Règles de preuve des actes sous seing privés

Les actes sous seing privés sont ceux qui ont été simplement conclus entre deux personnes privées, le cas échéant avec l'assistance d'un professionnel qui peut être le rédacteur de l'acte. La grande majorité des contrats les plus usuels font l'objet d'un acte sous seing privé.

Cas où un écrit papier ou son équivalent numérique est exigé

En droit français, les contrats civils portant sur une somme supérieure à 1500 euros doivent être prouvés par écrit (art. 1359 C. civ.). L'article 1365 du code civil prévoit que « *L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support* », ce qui englobe les écrits numérisés et le code informatique. L'article 1366 du code civil ajoute que « *l'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ». Pour qu'un écrit électronique soit assimilé à un écrit papier et que les exigences légales soient respectées, deux conditions sont posées: l'identification de l'auteur et la garantie du maintien de l'intégrité de l'acte. Sur une blockchain, le second point peut être considéré comme acquis. En revanche, la première condition renvoie à la problématique de la signature électronique évoquée plus bas (v. *infra* B) : si les exigences légales relatives à la signature électronique ne sont pas respectées, alors l'élément de preuve émanant d'une blockchain n'est pas assimilable à un écrit papier et la preuve du contrat conclu sur la blockchain n'est pas rapportée. En revanche si les modalités de signature électronique respectent les exigences légales, alors l'écrit électronique est réputé assimilé à un écrit papier.

L'écrit papier est parfois requis par des textes spéciaux relatifs à des contrats spécifiques (contrat d'édition, vente de fonds de commerce, cession de créance etc...) non pas à titre probatoire mais en tant que condition de fond. Il faut en ce cas également respecter les conditions précitées si l'on souhaite recourir à un support électronique, de manière à ce que l'écrit électronique se voit reconnaître la même portée que l'écrit papier.

Il faut signaler, à ce sujet, que l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse a introduit, dans le Code monétaire et financier, un article L. 223-13 qui prévoit que : « *Le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement électronique mentionné à l'article L. 223-12, qui tient lieu de contrat écrit pour l'application des articles 1321 et 1322 du code civil.* ». L'inscription de la cession dans un registre distribué (aux caractéristiques sont à préciser) est donc réputée tenir lieu de contrat écrit, ce qui constitue un changement notable d'avec le droit positif actuel. Les textes

d'application de cette ordonnance ne sont toutefois pas encore parus et devraient (logiquement) imposer le respect des conditions posées par l'article 1365 C. civ. (garantie du maintien de l'intégrité de l'acte et identification de l'auteur) ce qui renvoie, là encore, aux exigences relatives à la signature électronique qualifiée. Il est donc vraisemblable que les textes d'application n'admettent l'assimilation de l'inscription dans un DLT à un écrit que pour les plateformes faisant intervenir des tiers de confiance et permettant des signatures électroniques qualifiées. Il est donc, à cet égard, fort probable que ces plateformes soient relativement permissionnées et centralisées.

Cas où tout moyen de preuve est admis

L'exigence d'écrit ne concerne pas les contrats commerciaux (art. L110-3 C. com.) ou les contrats civils portant sur moins de 1500 euros. Sauf règles particulière, ces contrats bénéficient d'un principe de liberté de la preuve, ce qui signifie que tout moyen de preuve peut être employé pour les établir : présomptions, témoignages etc...

Il est donc possible de produire tous documents et éléments électroniques, même si ceux-ci ne remplissent pas les conditions requises par la loi pour être assimilés à de l'écrit papier. Ils seront librement appréciés par le juge, ce qui implique une certaine incertitude. Le plus vraisemblable est que le juge, en présence d'éléments de preuve provenant d'une blockchain, nommera un expert chargé d'apprécier la portée probatoire des différents éléments produits.

b) La signature électronique

La signature électronique sur la blockchain comporte des spécificités liées aux techniques cryptographiques particulières utilisées et notamment à l'articulation clé privée/clé publique (v. sur ce point, Paris Europlace, *Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché*, Rapport du groupe Fintech, 26 octobre 2017, pp. 84-90).

L'article 1367 du code civil prévoit que « *Lorsque [la signature] est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État* ». Il y a donc, ici, deux situations : soit l'on se trouve dans un cas de figure dans lequel la présomption de fiabilité de l'identification joue car les exigences réglementaires sont remplies, soit les conditions fixées par le décret ne sont pas remplies et la fiabilité est à l'appréciation du juge.

C'est désormais le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, pris en application du Règlement 910/2014 du Parlement européen et

du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit Règlement eIDAS, qui fixe les conditions requises pour la fiabilité d'un procédé. Ce décret dispose que *« la fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée. Est une signature électronique qualifiée :*

- *une signature électronique avancée,*
- *conforme à l'article 26 du règlement susvisé*
- *et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement. »*

Pour que la fiabilité d'une signature électronique sur la blockchain soit présumée, il faudrait donc non seulement que cette signature puisse être considérée comme une signature électronique *avancée* mais aussi qu'elle constitue une signature *qualifiée* ce qui suppose l'intervention d'un prestataire de service de confiance agréé, telle que le règlement eIDAS le prévoit.

Le règlement eIDAS distingue entre trois types de signatures électroniques, qui apparaissent déjà dans la Directive 1999/93/CE de 1999 : la signature simple, la signature avancée et la signature qualifiée. La signature électronique simple ne correspond à aucune spécificité technique et ne jouit pas d'une portée particulière en matière probatoire.

La signature *avancée* doit, en revanche, correspondre à quatre particularités techniques précisées par l'article 26 du règlement eIDAS :

- a) être liée au signataire de manière univoque ;
- b) permettre d'identifier le signataire ;
- c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif et
- d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Ces conditions paraissent remplies en présence d'une chaîne de blocs dès lors que des modalités sont mises en place afin que la condition c) soit respectée, ce qui implique que l'utilisateur ait, par exemple, le contrôle de sa clé privée grâce à un code personnel ou un mot de passe personnalisé lui conférant un contrôle exclusif. Il

reste que la signature *avancée* ne bénéficie pas d'une présomption de fiabilité, même si le juge devrait lui conférer une portée probatoire plus importante que la signature simple.

Pour pouvoir bénéficier de la présomption de fiabilité, la signature sur la blockchain doit constituer une signature *qualifiée*, ce qui signifie qu'elle doit remplir les conditions précitées pour constituer une signature avancée mais également être « *créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement* ». Cela signifie concrètement qu'il convient de recourir aux services de prestataires de service de confiance agréés afin d'obtenir des certificats qualifiés de signature électronique (v. annexes I et II du règlement).

En l'état actuel des choses, donc, les signatures sur la blockchain qui ne font pas intervenir de tiers certificateurs dans les conditions prévues par le règlement eIDAS ne bénéficient pas de la présomption de fiabilité. Dans le même temps, la signature blockchain constitue vraisemblablement une signature *avancée* au sens du règlement, ce qui est toutefois insuffisant pour faire de la signature blockchain l'équivalent d'une signature manuscrite. Par ailleurs, le recours à un tiers certificateur agréé, renchérit le coût de l'investissement dans la technologie blockchain et constitue précisément ce que les architectures distribuées doivent permettre d'éviter. Une telle situation n'est pas satisfaisante : il conviendrait ici que la blockchain permette, précisément, de s'affranchir du recours aux services d'un tiers certificateur tout en offrant une réelle sécurité juridique.

c) L'horodatage électronique

L'horodatage sur la blockchain est sûr une fois qu'il est intervenu, mais comporte une particularité propre à cette technologie, à savoir le fait qu'il n'est pas instantané (au moins 10 minutes sur la blockchain Bitcoin, voire plusieurs heures si le réseau est encombré). Il s'agit là d'une limite qu'il faut garder à l'esprit.

Le règlement eIDAS prévoit, dans son article 42, les exigences applicables aux horodatages électroniques qualifiés, qui bénéficient « d'une présomption d'exactitude de la date et de l'heure qu'il indique et de l'intégrité des données auxquelles se rapportent cette date et cette heure » (art. 41 Règlement préc.). Or l'horodatage électronique qualifié fait, lui aussi, intervenir un prestataire de service de confiance qualifié.

Les dispositions de droit interne vont dans le même sens. Le décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique prévoit que l'horodatage électronique est présumé fiable si le prestataire de service d'horodatage et le module d'horodatage utilisés satisfont à certaines

exigences qu'il précise. Il n'est donc pas possible à celui qui n'est pas un prestataire de service d'horodatage électronique qualifié au sens du décret de proposer un service d'horodatage électronique sur la blockchain qui bénéficie d'une présomption de fiabilité.

A défaut de respecter les spécificités requises par ces textes et de faire intervenir un prestataire qualifié, l'horodatage blockchain ne bénéficie pas d'une présomption d'exactitude ou de fiabilité et est librement apprécié par le juge. L'intervention d'un tiers certificateur constitue, là encore, une contrainte de nature à compliquer et surenchérir le coût de l'investissement dans la technologie blockchain. Il convient donc certainement d'adapter les règles relatives à l'horodatage sur la blockchain pour tenir compte de sa fiabilité.

2.2.2. Le cas particulier de l'acte authentique

L'acte authentique est, au contraire de l'acte sous signature privée, reçu par un officier public, en général un notaire. La force probatoire de l'acte authentique tient au fait qu'il « *fait foi jusqu'à inscription de faux* » (art. 1371 C. civ.). Cela signifie que le juge doit tenir pour vrai ce qui figure dans l'acte authentique : le contenu de celui-ci s'impose à lui car l'officier public l'a personnellement constaté.

Il est tentant de vouloir conférer l'authenticité aux transactions réalisées sur la blockchain, ce qui aboutirait à leur conférer une portée probatoire qui s'imposerait au juge jusqu'à « inscription de faux ». L'idée a déjà été envisagée. Un amendement déposé à l'Assemblée Nationale en 2016 prévoyait ainsi d'insérer, après le deuxième alinéa de l'article L. 330-1 du code monétaire et financier, un alinéa ainsi rédigé : « *Les opérations effectuées au sein d'un système organisé selon un registre décentralisé permanent et infalsifiable de chaîne de blocs de transactions constituent des actes authentiques au sens du deuxième alinéa de l'article 1317 du code civil. L'Autorité des marchés financiers habilite le système répondant aux conditions de sécurité et de transparence définies dans un décret pris en conseil d'État.* » (amendement n°CF2 déposé le 13 mai 2016 par Mme de la Raudière au projet de loi dit « Sapin 2 » relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique).

En principe, l'authenticité concerne les actes personnellement constatés par des personnes spécialement habilitées pour ce faire. Assimiler une transaction réalisée sur une blockchain à un acte authentique va sans doute au delà des besoins actuels, compte-tenu des cas d'usage pour l'heure envisagés. Si l'on souhaitait un jour réaliser sur la blockchain des transactions pour lesquelles la loi exige actuellement qu'un acte authentique soit dressé, il suffirait de renoncer simplement à l'exigence d'acte authentique. Par exemple, pour que les transactions immobilières soient, dans

le futur, réalisées sur la blockchain, il suffirait simplement de renoncer à exiger l'établissement d'un acte notarié pour pouvoir procéder à la publicité foncière.

Conférer l'authenticité à l'acte intervenu sur une blockchain n'apparaît donc pas, pour l'heure, indispensable. Relevons ici en passant que la question de la « force exécutoire », souvent soulevée à propos de l'exécution automatique des actes conclus sur une blockchain (en cas de *smart contract*), relève d'une autre problématique que celle de l'authenticité et du droit de la preuve (v. la fiche relative aux *smart contracts*).

2.2.3. La preuve d'un fait juridique sur une blockchain

En dehors des transactions réalisées sur la blockchain -qui constituent des actes juridiques- de simples faits juridiques extérieurs à la blockchain peuvent y être enregistrés.

Le cas des oracles

Lorsque le fait considéré s'est déroulé à l'extérieur du réseau, par exemple dans le monde physique (livraison d'une marchandise), l'information est entrée dans la blockchain manuellement, le plus souvent à l'aide d'oracles. Ce système d'oracles permet ainsi d'enregistrer dans la blockchain que telle marchandise a été livrée tel jour à telle heure (ce qui repose la question de la portée de l'horodatage évoquée plus haut).

Une fois que l'information est entrée dans la blockchain, il n'est plus possible de la modifier ou la falsifier. Il reste que sa fiabilité est entièrement dépendante de la confiance que l'on peut avoir dans l'oracle. Il existe actuellement plusieurs systèmes d'oracles en cours de perfectionnement. Il apparaît délicat de conférer, pour l'heure, une portée probatoire renforcée aux informations transmises par les oracles dès lors que la technologie employée n'apparaît pas encore mature ni totalement dépourvue de failles de sécurité.

Le juge appréciera donc souverainement la portée probatoire des éléments issus d'une blockchain et versés afin d'établir de tels faits juridiques. En cas de contestation, il désignera probablement un expert et se penchera sur les autres indices dont il dispose.

La blockchain comme registre

L'élément extérieur que l'on cherche à enregistrer dans la blockchain peut ne pas être un événement du monde physique mais un fait d'un autre ordre : création d'une œuvre originale ou obtention d'un diplôme, par exemple. En ce cas la fonction de hashage permet de s'assurer que l'œuvre ou le diplôme considéré n'est pas altéré

ou modifié. Ici, la technologie blockchain présente l'avantage considérable de faire en sorte que l'intégrité de ces éléments enregistrés et horodatés est garantie.

Couplée à des outils de stockage, la blockchain peut ainsi servir de registre numérique infalsifiable pour un très grand nombre de documents. L'expérimentation de la blockchain dans le cadre de la dématérialisation des registres d'état civil a ainsi été envisagée par deux amendements déposés dans le cadre des discussions relatives au projet de loi sur l'Etat au service d'une société de confiance (amendements n°385 et n°755 du 19 janvier 2018) actuellement discuté au Parlement. Il est certainement regrettable que ces amendements aient été, pour l'heure, rejetés, même si l'hypothèse d'un recours à la blockchain pour les registres d'état civil n'est pas écartée pour autant.

Il serait, en tout état de cause, souhaitable que le droit français reconnaisse pleinement la fiabilité de la conservation de documents originaux au moyen de la technologie blockchain. Or les documents électroniques correspondant à l'empreinte numérique enregistrée sur la blockchain remplissent, sans aucun doute, les conditions prévues par l'article 1379 du Code civil concernant les copies. L'article 1379 alinéa 2 du Code civil prévoit en effet qu'est « *présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'Etat* ». Et la technologie blockchain correspond aux exigences posées par le décret d'application [n°2016-1673 du 5 décembre 2016](#), qui prévoit notamment, dans son article 3, que « *l'intégrité de la copie résultant d'un procédé de reproduction par voie électronique est attestée par une empreinte électronique qui garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable* ». Il n'apparaît donc pas que le droit positif doive substantiellement être modifié ici, si ce n'est, peut-être, pour intégrer dans le texte du décret une disposition propre à la blockchain prévoyant expressément que le recours à cette technologie permet, si certaines conditions techniques sont respectées, d'obtenir des copies fiables.

Il reste toutefois, là encore, et malgré la confiance que l'on peut accorder aux techniques cryptographiques mises en œuvre sur la blockchain, à s'assurer que le document numérique dont l'empreinte est enregistrée sur la plateforme correspond bien au document original. Il paraît difficile, à ce stade, d'envisager une autre solution que celle de l'intervention d'un tiers de confiance, sauf dans le cas où c'est l'émetteur du document (l'Etat pour les actes d'état civil, l'école pour les diplômes etc...) qui procède lui-même à son inscription sur une blockchain. Certaines start up proposant l'enregistrement d'œuvres originales sur la blockchain prévoient ainsi l'intervention, en cas de contestation, d'un huissier chargé d'attester que le document écrit ou

électronique initial et son empreinte numérique enregistrée sur la blockchain sont identiques.

En tout état de cause, il n'apparaît pas que ce cas d'usage appelle une évolution du droit de la preuve en tant que tel si ce n'est pour rendre opposable l'horodatage réalisée sur la blockchain lors de l'enregistrement de l'empreinte numérique du document.

3. Propositions

Les exigences actuelles en matière probatoire (signature et horodatage *qualifiés*) sont extrêmement contraignantes en ce qu'elles imposent le recours à un tiers certificateur, sans lequel on ne peut présumer la fiabilité de l'identification du signataire ou de l'exactitude de l'horodatage. Une incertitude en résulte, car le juge sera libre d'apprécier ces éléments de preuve comme il le souhaite. Il est vraisemblable qu'il désignera un expert à cette fin, ce qui aura pour effet d'allonger et renchérir le coût des procédures.

Il conviendrait donc certainement de modifier les textes existants à ce sujet afin de faire en sorte que la signature et l'horodatage intervenus sur une blockchain répondant à des spécifications techniques satisfaisantes bénéficient de la présomption de fiabilité.

Sur le fond et dans la longue durée, il apparaît donc souhaitable que les règles eIDAS évoluent afin de tenir compte des spécificités techniques de la technologie blockchain auxquelles les textes existants ne sont actuellement pas adaptés. Il conviendra de déterminer les conditions permettant de reconnaître une plus grande portée probatoire à la signature électronique et à l'horodatage intervenus sur la blockchain. La réflexion devrait être entamée à ce sujet au niveau européen. Et il faudra, à cet égard, déterminer les caractéristiques techniques justifiant d'accorder la présomption de fiabilité, étant précisé qu'il n'apparaît pas souhaitable d'aller au-delà d'une simple présomption réfragable, compte-tenu des difficultés pouvant toujours survenir (vol de clé privée etc...).

Dans cette attente, le droit interne pourrait lui-même évoluer de manière à donner une portée renforcée à la preuve émanant d'un registre distribué présentant des caractéristiques techniques satisfaisantes, sans pour autant imposer un recours redondant et onéreux à un tiers certificateur.

S'agissant de la signature électronique sur la blockchain, qui constitue une signature avancée au sens du Règlement eIDAS, il paraît difficile de présumer sa fiabilité en droit interne sans contredire le Règlement. Il serait néanmoins possible de travailler de concert avec l'ANSSI pour déterminer des modalités techniques d'identification particulièrement fiables et dont le juge pourrait tenir compte. Cette démarche devrait également être menée à propos de l'horodatage.

Par ailleurs, s'agissant des prestataires de confiance agréés actuellement habilités à délivrer certificats et cachets, il serait souhaitable d'entamer une réflexion en collaboration avec l'ANSSI afin d'obtenir des retours d'expérience et d'élaborer des bonnes pratiques.

Enfin, les transactions conclues au moyen de signatures avancées sur la blockchain pourraient se voir conférer une portée probante renforcée en étant, par exemple, qualifiées de commencements de preuve par écrit au sens de l'article 1362 du Code civil.

Recommandations

Nous recommandons :

- d'engager dès maintenant une réflexion devant aboutir à la révision du règlement eIDAS afin de reconnaître pleinement la fiabilité de la signature électronique et de l'horodatage sur la blockchain sans intervention d'un tiers certificateur ainsi que la fiabilité des algorithmes de signature issus des blockchains, même dans une utilisation isolée ;
- de réfléchir, dans cette perspective, aux modalités techniques devant être retenues afin de pouvoir reconnaître une pleine force juridique à la signature juridique et à l'horodatage réalisés sur une blockchain ou sur une chaîne ou structure de données satellite (dite « sidechain », ou « arbre de Merkle »), dont la force probante découle de la blockchain principale ;
- d'impliquer l'ANSSI de manière à faire apparaître de bonnes pratiques concernant « l'offre blockchain » actuellement développée par les tiers certificateurs agréés ;
- d'adopter dès à présent une réforme visant à renforcer la force probante des informations figurant sur une blockchain selon des modalités techniques à préciser. L'article 1362 du Code civil pourrait, par exemple, se voir ajouter un quatrième alinéa prévoyant que « l'écrit électronique enregistré dans un dispositif d'enregistrement électronique partagé répondant à des caractéristiques prévues par décret en Conseil d'état tient lieu de commencement de preuve par écrit ».



Fiche 4

Fiscalité

Responsable de rédaction
Antoine Gabizon, avocat associé, Fieldfisher LLP

1. Contexte : un secteur en croissance sans cadre adapté

À ce jour, les règles énoncées ciblant spécifiquement la technologie blockchain visent uniquement le bitcoin et portent sur le traitement fiscal des gains et de la TVA.

Il eût été étonnant que le développement exponentiel des activités sur la blockchain, la capacité accrue de procéder à des opérations libellées en monnaie virtuelle, l'attrait des opérations d'ICO, l'émission de ces objets non identifiés juridiquement que sont les « *tokens* » (ou jetons émis sur la blockchain par les opérateurs sur le système) n'apporte pas son lot d'interrogations d'un point de vue fiscal.

C'est d'autant plus crucial pour les États que le volume financier des opérations concernées ne cessent lui-même de croître et que s'agissant d'activités qui sont à la fois décentralisées territorialement, digitalisées et qui s'exécutent de manière automatique au travers de *smart contract*, la déperdition de profits taxables pourrait prendre une ampleur encore plus importante que ce que l'on connaît actuellement avec l'usage d'internet.

Pour les entreprises qui développent cette nouvelle activité, l'incertitude fiscale qui règne sur leurs activités dans la majorité des pays développés est une source d'inquiétude. Cette inquiétude est d'autant plus grande qu'elle se double de la forte volatilité des cryptomonnaies, parfois d'un manque de liquidité, ainsi que de l'insécurité qui pèse sur les clés informatiques supposées garantir la détention de ces actifs. Cette situation pousse les opérateurs soit à adopter des positions qui pourraient s'avérer excessivement prudentes et de nature à ralentir leur développement, ou, à l'inverse à chercher à délocaliser leurs activités vers des pays dont la réglementation apparaît de nature à sécuriser le traitement fiscal.

Prenant conscience du succès grandissant du bitcoin, l'administration fiscale a donc édicté en juillet 2014 un certain nombre de principes destinés à en définir le régime fiscal. Cependant, les nouvelles activités qui se sont développées autour de la

blockchain ont considérablement évoluées depuis la parution de ces commentaires. En effet, ces commentaires ne nous éclairent pas sur les échanges de cybermonnaies ni sur l'émission de *tokens* dans le cadre d'une ICO, qui permet de financer des sociétés en utilisant des *smart contracts* sur la blockchain.

La sécurisation du traitement fiscal des activités se développant autour de la blockchain est un enjeu considérable pour l'attraction de projets innovants en France s'appuyant sur cette nouvelle technologie.

2. État des lieux : des règles incomplètes, sources d'incertitudes

2.1. Personnes physiques réalisant des gains à titre occasionnel

Les gains provenant de la revente de bitcoins sont, d'après l'administration, taxables dans la catégorie des bénéfices non commerciaux (BNC)¹.

Ces commentaires excluent l'application de l'article 150 UA du Code général des impôts (CGI) relative au traitement des plus-values sur biens meubles réalisées par un particulier non professionnel. Pourtant, en matière professionnelle, l'administration reconnaît que l'achat-revente de bitcoins est assimilable à une activité d'achat-revente de biens meubles incorporels. Son analyse n'est donc pas cohérente avec la qualification qu'elle retient en matière de BIC.

De plus, il n'est pas certain que ces commentaires trouvent à s'appliquer en présence d'autres cybermonnaies que le bitcoin, dès lors que la doctrine administrative est d'interprétation stricte.

Par ailleurs, les commentaires posent également difficulté dans le cas d'échanges entre cybermonnaies (par exemple des échanges de bitcoins contre des ethers). Dans cette situation, une interprétation prudente des commentaires administratifs conduit à la constatation d'un produit taxable, bien que la situation ne soit pas expressément visée.

Cette position nous paraît également critiquable au regard de la notion de revenu disponible. Les risques liés à la sécurité, à la liquidité et à la volatilité des cybermonnaies fragilisent la constatation d'un revenu disponible entre les mains du particulier, au sens de l'article 156 du CGI.

Enfin, la constatation d'un profit taxable évaluée à la date de l'échange peut amener le contribuable à supporter une charge d'impôt sans qu'il ait les fonds pour y faire face et alors même qu'il n'a aucune garantie sur la pérennité de ce gain virtuel.

¹ Doctrine administrative BOI-BNC-CHAMP-10-10-20-40, n° 1080.

Cela étant, l'administration fiscale pourrait naturellement objecter que ce constat est propre en réalité à toute opération d'échange de biens qui ne comporte pas, par définition, de flux financiers.

2.2. Personnes, physiques ou morales, exerçant une activité à titre professionnel

Pour les personnes, morales ou physiques, exerçant une activité d'achat-revente de bitcoin à titre professionnel, les commentaires ne fournissent qu'un éclairage partiel sur le traitement de ces opérations et de nombreuses interrogations subsistent¹.

L'achat-revente de bitcoins à titre habituel est considéré comme une activité commerciale relevant de la catégorie des bénéfices industriels et commerciaux.

Ces précisions ne fournissent que très peu de réponses aux problématiques rencontrées par les entreprises utilisant les cybermonnaies.

En particulier, les commentaires n'envisagent pas clairement les opérations réalisées en cybermonnaie. Il s'agit notamment des acquisitions de biens ou services par un paiement en cybermonnaie mais également des opérations d'échanges (bitcoins contre ethers, par exemple) y compris dans le cadre de ventes de tokens, l'échange (de bitcoins, ethers ou autres) contre des tokens dont on sait qu'ils peuvent avoir des caractéristiques très diverses décidées par son émetteur.

En l'absence de précisions, l'application des principes énoncés à l'article 38 du CGI sur le bénéfice imposable conduit en principe à traiter ces opérations comme des échanges de biens.

Cette situation peut se révéler très délicate pour les entreprises qui peuvent alors faire apparaître un bénéfice imposable significatif sans être en mesure de faire face à l'impôt correspondant dès lors que l'impôt s'y rapportant ne peut, par hypothèse, pas être acquitté en cybermonnaie et que la capacité de conversion des actifs concernés en monnaie légale peut ne pas être suffisante à date de paiement du solde de l'impôt et du versement des acomptes d'impôts sur les sociétés.

Une telle solution pose également des problèmes sur le plan comptable, au regard des principes généraux édictés par le Plan comptable général (PCG) et notamment le principe comptable de continuité d'exploitation et le principe de bonne information. En effet, les commissaires aux comptes rencontrent des difficultés pour la certification des comptes de sociétés ayant un volume important de cybermonnaies, en raison de leur très forte volatilité et du manque de liquidité de ces biens. Il a pu notamment être considéré que certains tokens en fonction de leurs caractéristiques

¹ Doctrine administrative BOI-BIC-CHAMP-60-50, n° 730.

ne répondent pas à la définition d'un actif dont la valeur est déterminable de façon suffisamment fiable ou d'une créance certaine à faire figurer à l'actif. Dans ces situations, les professionnels comptables (experts-comptables et commissaires aux comptes) envisagent l'enregistrement d'un engagement hors bilan.

Sans même en arriver à de telles extrémités, dans la lignée de la jurisprudence de la Cour de justice de l'Union européenne et à défaut de règle comptable spécifique, les cybermonnaies pourraient être comptabilisées comme un moyen de paiement et voir alors s'appliquer les règles propres aux avoirs ou créances en monnaie étrangère.

Or l'article 38,4 du CGI impose leur évaluation à la clôture de chaque exercice et la constatation des écarts de change pour la détermination du résultat fiscal.

Certes, une éventuelle parade consiste à considérer que ces règles ne peuvent être appliquées dans le cas des cybermonnaies dans la mesure où il ne s'agit pas de monnaie ayant cours légal. Mais cette analyse reste incertaine en l'état de la réglementation.

Une comptabilisation en tant qu' « autres immobilisations financières » (qui suppose un investissement dans la durée) ou en tant que stocks (dans le cas des sociétés qui poursuivent un but spéculatif) est alternativement envisageable, mais dans l'attente des recommandations des autorités comptables, elle reste également aléatoire.

Enfin, la très forte volatilité du cours peut conduire l'entreprise à voir disparaître la presque totalité de son patrimoine instantanément et ne plus être en mesure de faire face aux impositions dues, ce qui de facto entraîne des conséquences pour les commissaires aux comptes et notamment une procédure d'alerte du président du Tribunal de commerce conformément aux dispositions du Code de commerce.

2.3. L'activité de minage

Le minage est défini par l'administration comme l'activité qui consiste à contribuer de la puissance de calcul au réseau afin qu'il fonctionne et soit sécurisé en contrepartie de l'attribution de bitcoins.

L'administration considère que l'attribution de ces bitcoins est faite à titre gratuit et exclut une imposition au moment de l'attribution. Une telle règle n'allait pas de soi. Non seulement car le minage est une activité qui a un coût (matériel informatique et électricité dépensée) mais également parce qu'elle conduit à reporter la taxation au moment de l'utilisation du bitcoin soit par une conversion contre une monnaie ayant cours légal, soit par un échange contre des biens et des services.

Cette solution est salubre en ce qu'elle ne pénalise pas le mineur en le forçant à vendre une partie de ses gains pour pouvoir payer l'impôt.

On peut souhaiter qu'une telle solution soit étendue aux autres cybermonnaies et plus généralement aux échanges entre cybermonnaies, en reportant la taxation du profit au moment de l'utilisation des cybermonnaies contre des biens (à l'exclusion d'autres cybermonnaies) ou services ou lors de leur conversion en monnaie *fiat*.

2.4. En matière de droits de mutation à titre gratuit et d'impôt sur la fortune

Nous précisons en premier lieu que l'impôt sur la fortune (ISF) a été supprimé à compter du 1^{er} janvier 2018 par le projet de loi de finances pour 2018 et est remplacé par un impôt qui n'inclut pas dans sa base les bitcoins et autres cybermonnaies.

Cependant, les difficultés soulevées en matière de valorisation appellent à une réponse en matière de mutations à titre gratuit.

L'administration précise que les « unités de compte virtuelles stockées sur un support électronique », font partie du patrimoine taxable du contribuable ou du défunt¹.

Nous noterons que cette fois-ci, la définition est plus large et ne se limite pas au cas spécifique du bitcoin.

La valorisation est un sujet délicat pour les raisons déjà précédemment évoquées : les problèmes de liquidités pour cybermonnaies, leur forte volatilité ou encore les risques en matière de sécurité et de pérennité du patrimoine qu'elles représentent.

Des commentaires de l'administration sur les méthodes de valorisation prenant en compte ces facteurs seraient appréciables.

2.5. En matière de TVA

L'administration n'a, à ce jour, apporté aucune précision sur le traitement des opérations réalisées en cybermonnaies. Sans entrer dans les détails, c'est la Cour de justice de l'Union européenne (CJUE, 22 octobre 2015, aff. C-294/14, Hedqvist) qui a été amené à préciser implicitement que sont exonérés de TVA les opérations d'échange de bitcoins contre des devises ayant cours légal dès lors que les bitcoins sont assimilables à des devises (moyen de paiement) au sens de la directive TVA.

Les opérations d'échange de bitcoins contre des monnaies ayant cours légal sont donc exonérées de TVA en application de l'article 261 C, 1-d du CGI en France.

Les opérations concernant les cybermonnaies présentant les mêmes caractéristiques (ethers notamment) devraient donc suivre le même raisonnement et relever de l'exonération prévue en France à l'article 261 C, 1-d du CGI. La poursuite

¹ Doctrine administrative BOI-ENR-DMTG-10-10-20-10, n° 10 et BOI-PAT-ISF-30-20-10, n° 80.

du raisonnement nous amène donc à exonérer de TVA les opérations d'échanges réalisées entre certaines cybermonnaies ayant ces caractéristiques (par exemple, vente de bitcoins contre des ethers).

Pour autant, l'incertitude demeure pour les autres tokens dont on sait qu'ils peuvent recouvrir des réalités très différentes.

3. Recommandations

Pour clarifier le régime fiscal des gains en cybermonnaies et autres tokens, le groupe de travail formule les propositions suivantes.

3.1. Pour les particuliers réalisant des gains à titre occasionnel

S'agissant de la taxation des revenus, plusieurs solutions peuvent être envisagées.

Une première solution, qui a le mérite de ne pas nécessiter l'intervention du législateur, serait de reconnaître que les gains en cybermonnaie correspondent à des plus-values sur biens meubles soumises au régime de l'article 150 UA du CGI.

L'application de ce régime permettrait notamment aux particuliers d'être exonérés lorsque leur prix de cession ne dépasse pas 5 000 € et d'être imposés sur une base forfaitaire dans les autres cas (au taux de 19 % auquel il convient d'ajouter les contributions sociales).

Nous devons constater qu'un tel régime semble plus adapté aux gains de cybermonnaies réalisés à titre occasionnel que le régime de déclaration d'un revenu d'activité en BNC préconisé par l'administration pour les gains tirés de la vente de bitcoins.

En effet, on comprend mal ce qui permet automatiquement d'exclure ces gains du régime des gains en capital. L'application du régime des bénéfices non commerciaux conduit à une taxation lourde des contribuables ayant réalisé des plus-values en revendant leurs cybermonnaies, comme s'il s'agissait de revenus d'activité et non d'un gain en capital. Alors que le gouvernement allège considérablement la fiscalité du capital, un tel régime pour les plus-values sur la cybermonnaie apparaît excessivement sévère.

Il faudrait alors selon nous rapporter la doctrine administrative relative au traitement des bitcoins dans la catégorie des bénéfices non commerciaux. Cela conduirait à l'application d'un taux forfaitaire de 19 %, auxquels s'ajouteraient les prélèvements sociaux au taux de 17,2 % (à compter du 1^{er} janvier 2018).

Une autre solution serait d'inclure ces gains dans le champ du prélèvement forfaitaire unique de 30 % prévue par la loi de finances pour 2018.

Cette solution nous semble particulièrement justifiée dans la mesure où, dans la plupart des cas, les tokens sont émis par l'intermédiaire d'une ICO en vue de financer l'activité de jeunes sociétés et peuvent donc s'apparenter à un investissement contribuant au développement d'un secteur économique porteur, bien qu'ils n'aient pas les mêmes contreparties ni ne confèrent les mêmes droits qu'une part dans une société. L'un des objectifs affichés du gouvernement étant de favoriser l'investissement par des mesures incitatives et par la simplification des régimes fiscaux, l'extension du champ du prélèvement forfaitaire unique aux gains de cybermonnaies pourrait tout à fait s'inscrire dans ce cadre.

Ceci nécessitera d'assimiler les gains sur actifs numériques à des plus-values sur cession de biens meubles incorporels tels que définis à l'article 150-0-A du CGI.

À l'appui de ces propositions, il n'est pas inutile de souligner qu'elles sont globalement cohérentes avec les niveaux d'imposition constatés dans d'autres pays. Ainsi, sous réserve des incertitudes qui peuvent apparaître à raison de cadres législatifs relativement imprécis, on constate les pratiques suivantes (dans le cas des revenus considérés comme non spéculatifs uniquement) :

États	Taux d'imposition
Allemagne	Imposition au titre des plus-values privées au taux de 25%
États-Unis	Régime des plus-values à long terme : application d'un taux marginal de 20 %
Israël	Imposition au titre des plus-values privées au taux forfaitaire de 25%
Italie	Pas d'imposition en l'état de la réglementation
Royaume-Uni	Imposition pour un investisseur au taux forfaitaire de 28%

S'agissant des échanges entre cybermonnaies (par exemple bitcoins contre des ethers ou d'autres tokens), des précisions de l'administration seraient les bienvenues afin de confirmer l'analyse selon laquelle les gains latents de cybermonnaie ne constituent pas un revenu disponible du contribuable, au sens de l'article 156 du CGI. L'imposition serait alors reportée et n'interviendrait qu'au fur et à mesure de l'utilisation des cybermonnaies pour l'acquisition de biens (autres que des cybermonnaies) ou de services.

3.2. Pour les opérations commerciales en cybermonnaies

En ce domaine, une première solution serait de savoir si, dans l'attente de pouvoir disposer de principes précis en ce domaine, il serait fiscalement acceptable de considérer que les opérations d'échanges entre cybermonnaies puissent être comptabilisées en engagement hors bilan. Les actifs numériques ne seraient donc imposables qu'au fur et à mesure de leur utilisation contre des achats de biens ou de services de toute nature, ou bien encore de leur conversion en monnaie légale, à l'exception toutefois des conversions vers d'autres cybermonnaies. Cette solution de court terme n'est cependant pas adaptée à une appréhension complète et cohérente des actifs numériques par la fiscalité. Ceci d'autant plus que les arguments qui militent pour cette solution d'un point de vue comptable ne sont pas à l'abri de toute critique.

Une autre solution serait de préciser le champ d'application des commentaires de la doctrine administrative applicable en matière de bénéfices industriels et commerciaux et de bénéfices non commerciaux qui devrait conduire à reporter la taxation du produit des opérations réalisées en bitcoin (ou tout autre unité de valeur comparable) au moment de leur utilisation pour l'achat de biens ou de services ou encore leur conversion en monnaie légale. Dans ce cas, la valeur inscrite en comptabilité serait neutralisée extra-comptablement. Cette solution trouverait notamment à s'appliquer aux opérations d'échanges de cybermonnaies en matière d'ICO (échange de tokens émis par la société contre des bitcoins et autres cybermonnaies) en reportant la taxation des cybermonnaies reçus en échange des tokens au moment de leur conversion en monnaie légale ou de leur utilisation pour l'achat de biens ou de services.

Alternativement, une solution plus sécurisante que la précédente car inscrite dans la loi mais aboutissant in fine à un résultat comparable serait d'étendre le mécanisme de report d'imposition prévu à l'article 38-6 du CGI relatif à certains dérivés de crédit, qui permet de reporter l'imposition du profit constaté sur une position au dénouement de l'opération, le cas échéant en prévoyant une période maximale dans le temps. Le débouclage interviendrait à nouveau au moment de l'achat de biens ou de services ou encore de la conversion de la cybermonnaie en monnaie légale.

Il n'est toutefois pas certain que l'administration fiscale accepte d'adhérer à ces solutions dans la mesure où elles pourraient être perçues comme emportant un traitement fiscal plus favorable que celui tenant d'une simple clarification. Elles ne pourraient s'envisager qu'à la condition que le pouvoir législatif et l'administration fiscale acceptent de considérer que le développement de ces nouvelles activités mérite d'être soutenu sur le plan fiscal.

Une autre solution, peut-être plus réaliste et compatible avec les objectifs et les contraintes budgétaires de l'administration, serait de considérer que les opérations

réalisées en cybermonnaies sont imposables sur la base de leur contre-valeur au jour de réalisation des opérations ou de leur inscription au bilan mais de confirmer que les avoirs détenus ensuite en cybermonnaies échappent à la règle de taxation des écarts d'évaluation prévue à l'article 38,4 du CGI, s'agissant de moyens de paiement qui n'ont pas de cours légal au sens de ces dispositions.

3.3. En matière de TVA

En matière de TVA, deux options semblent pouvoir être envisagées.

Une première solution consisterait à confirmer et étendre le principe d'exonération des échanges de cybermonnaies contre des euros à toutes les opérations d'achat, vente ou échange d'actifs numériques. L'administration confirmerait alors l'application de la solution retenue par la CJUE assimilant les bitcoins à un moyen de paiement à tous les échanges entre cybermonnaies et l'appliquerait aux émissions et aux échanges de tokens en cybermonnaies, ainsi qu'aux échanges de tokens entre eux. Cette solution trouverait notamment à s'appliquer en matière d'ICO.

Mais, comme on l'a indiqué, cette solution présente une incertitude en tant que les tokens recouvrent des qualifications et des situations juridiques multiples, de sorte que leur assimilation à des moyens de paiement purs et simples n'est pas systématique.

Une seconde approche, plus complexe, serait de transposer aux émissions de tokens les principes énoncés par l'administration fiscale pour les émetteurs de bons cadeaux ou la commercialisation de monnaie numérique.

Dans ces deux hypothèses, l'administration fiscale indique que la simple émission de ces bons ou des supports de paiement (cartes, tickets, bons prépayés, etc.) permettant l'achat de produits ou de services n'est pas soumise à la TVA. C'est l'utilisation des bons qui déclenche la taxation dans la mesure où au moment de l'émission, la nature exacte des prestations ou des biens que le bénéficiaire choisira ultérieurement d'obtenir contre la remise de ceux-ci n'est pas connue, tout comme ne sont pas déterminés la date de réalisation de ces prestations ou livraisons de biens et les fournisseurs chargés d'en assurer l'exécution (cf. rescrit du 18 septembre 2007, n° 2007/31 TCA ; BOI-TVA-CHAMP-10-10-10, n° 80 et suivants, et lettre DLF du 20 mai 2009).

Dans la perspective de la directive européenne visant à harmoniser les règles concernant le régime de TVA applicable aux bons afin de garantir un régime fiscal uniforme dans l'ensemble des États membres qui doit entrer en vigueur à compter du 1^{er} janvier 2019 (directive 2016/1065/UE), cette solution conduirait à placer par anticipation les tokens dans le régime de taxation des bons à usages multiples qui se définissent comme des bons dont on ne connaît pas l'usage précis au moment de

leur émission. Selon la directive, l'imposition de ces bons à la TVA n'est prévue qu'au moment de la remise matérielle au fournisseur ou au prestataire du bien ou des services qu'ils servent à acquérir.

Ce raisonnement devrait s'appliquer à certains tokens qui permettent l'achat de biens ou de services, sans que l'on connaisse précisément leur sort définitif au moment de l'émission.

En tout état de cause, les opérations au cours desquelles ces actifs numériques (cybermonnaies ou tokens) seraient utilisés en paiement de prestations ou d'achats de biens seraient naturellement soumises à TVA dans les conditions de droit commun.



Fiche 5

Enjeux de conformité et droit au compte

Responsable de rédaction

Arnaud Grünthaler, avocat associé, Fieldfisher LLP

Une véritable problématique d'accès à un compte bancaire

Les établissements de crédit en France sont soumis à une obligation de lutte contre le blanchiment et le financement du terrorisme (« KYC-AML »), qui se traduit notamment par l'obligation d'identification de leur client ainsi que de l'origine des fonds d'un client, en particulier lors de la réalisation d'une transaction sur un compte bancaire.

Aux termes de l'article L. 561-2 du Code monétaire et financier (issu de l'article 2 de l'Ordonnance n° 2016-1635 du 1^{er} décembre 2016), « toute personne qui, à titre de profession habituelle, soit se porte elle-même contrepartie, soit agi en tant qu'intermédiaire, en vue de l'acquisition ou de la vente de tout instrument contenant sous forme numérique des unités de valeur non-monétaire pouvant être conservées ou être transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur ».

Il est donc considéré que les émetteurs de *tokens* et les professionnels achetant et revendant des cybermonnaies sont soumis à une obligation de lutte contre le blanchiment et le financement du terrorisme et doivent, de ce fait, identifier les acheteurs des tokens ou cybermonnaies ainsi que l'origine des fonds utilisés.

Cependant, en pratique, nous constatons que les émetteurs de tokens ou les vendeurs professionnels de cybermonnaies ont la plus grande difficulté à ouvrir et maintenir ouvert un compte bancaire classique auprès d'un établissement de crédit en France dans le cadre de leur activité. Ces difficultés apparaissent dès la constitution des sociétés émettrices lorsque les projets de statuts adressés à la banque mentionnent un objet lié à une activité faisant référence à la cybermonnaie. Cette problématique s'entend également à l'ensemble des entreprises gérant des cybermonnaies ou tokens dans le cadre de leur activité générale, soit parce qu'elles

l'acceptent comme moyen de paiement, soit parce que ces actifs numériques sont intégrés à leur offre de produit.

Pour bon nombre d'entre elles, les établissements bancaires auxquels elles s'adressent refusent les ouvertures de compte, arguant que ces activités sont dangereuses. Dans certains cas, les établissements acceptent des fonds mais les bloquent instantanément au motif que ces sociétés ne sont pas en mesure de respecter leurs obligations en matière de KYC-AML en l'absence d'identification précise de leur origine.

Cette problématique naît principalement du fait que les matrices de risques et autres procédures internes appliquées par les établissements bancaires dans le cadre de leurs propres obligations de lutte contre le blanchiment et le financement du terrorisme n'intègrent pas les cybermonnaies à leur cadre d'analyse. En pratique, la méconnaissance des cybermonnaies et autres actifs numériques par certains de ces départements conduit les établissements bancaires à refuser automatiquement de gérer les comptes des entreprises ayant des cybermonnaies à leur patrimoine, ayant organisé une opération de vente de tokens (ICO) ou plus simplement les utilisant dans le cadre de leur activité.

Or, l'une des raisons pour laquelle les banques sont parfois conduites à clôturer des comptes bancaires tient au caractère largement insuffisant des données que les plateformes d'échange fournissent aujourd'hui à leurs clients. Il est en pratique très difficile d'obtenir de ces plateformes des documents unifiés permettant de justifier d'opérations d'achat ou de vente précises. En l'absence de ces documents, les banques sont conduites à considérer que l'origine des fonds n'a pas pu être démontrée.

Les émetteurs de *tokens* ainsi que les acheteurs-revendeurs de cybermonnaies doivent alors trouver des alternatives en tentant d'ouvrir des comptes bancaires auprès de prestataires étrangers (banques ou prestataire de services de paiement) ou en immatriculant les sociétés faisant référence à un objet social générique sans préciser l'utilisation de cybermonnaies. Ces solutions temporaires ne règlent pas davantage le problème de fond, et dans le second cas un blocage ultérieur des fonds est commun lors du fonctionnement effectif du compte.

Un tel blocage est préjudiciable au développement du marché français et à l'attractivité de la place de Paris pour toute activité liée au commerce ou à l'utilisation de cybermonnaies ou de *tokens* dans la mesure où les alternatives envisagées sont systématiquement recherchées en dehors de France.

Recommandations

Une obligation d'information devrait être imposée aux entreprises gérant des plateformes d'échanges, qui auraient à fournir un état des achats/vente permettant aux particuliers de justifier de l'origine des fonds utilisés dans le cadre de transactions sur cybermonnaies. Dans le cas de vente de tokens, ce *reporting* permettrait également aux émetteurs de satisfaire leur propre obligation de KYC-AML et de satisfaire le KYC des banques en fournissant cette information communiquée par les exchanges aux souscripteurs de tokens.

Dès lors, une information des banques pourrait lever des ambiguïtés et la prise en compte effective des mesures développées par les émetteurs de *tokens* et vendeurs de cybermonnaies.

Les émetteurs de *tokens* pourraient également avoir recours aux services de prestataires spécialisés qui permettent une identification des souscripteurs dans le cadre d'une vente de ces *tokens* et qui réalisent les diligences techniques d'un KYC-AML. L'utilisation de tels prestataires de services pourrait conforter les banques dans la réalisation par les émetteurs d'un KYC-AML et de fait permettre aux banques de satisfaire leurs propres obligations en la matière lors du transfert de fonds des exchanges vers les comptes bancaires classiques des émetteurs.

Rédacteurs du rapport juridique

Rédacteurs principaux

Simon Polrot, directeur exécutif, [Variabl](#)

Hélène Lefebvre, avocat associé, [Fieldfisher LLP](#)

Anne-Hélène Le Trocquer, avocat associé, [De Gaulle Fleurance & Associés](#)

Xavier Lavayssière, directeur, [ECAN](#), Smart Contract Academy

Florence G'sell, professeur de droit, université de Lorraine

Antoine Gabizon, avocat associé, [Fieldfisher LLP](#)

Arnaud Grunthaler, avocat associé, [Fieldfisher LLP](#)

Contributeurs signataires

Alain Roset, R & D, [La Poste](#)

Alexandre Stachtchenko, cofondateur, [Blockchain Partner](#)

Claire Leveneur, doctorante en Blockchain et droit privé, université Paris 2 Panthéon-Assas

Clément Lesaege, directeur de la technologie, [Kleros](#),

Fabrice Heuvrard, commissaire aux comptes et expert-comptable, cabinet Fabrice Heuvrard

Georgie Courtois, avocat associé, [De Gaulle Fleurance & Associés](#)

Hubert de Vauplane, avocat associé, [Kramer Levin LLP](#)

Jean-Michel Pailhon, vice-président, [Ledger](#),

Laurent Henocque, président, KeeeX, <https://keeex.me>

Luc Grynbaum, avocat, professeur, [De Gaulle Fleurance & Associés](#),

Michelle Abraham, avocat associé, chargée de cours, [cabinet Michelle Abraham](#)

Primavera De Filippi, chercheuse, CERSA/CNRS

William O'Rorke, juriste, [Blockchain Partner](#)



ANNEXES



ANNEXE 1

LETTRÉ DE MISSION



Paris, le 27 AVR. 2017

Le Commissaire général

Objet : groupe de travail sur les enjeux des « blockchains »

Madame la Professeur,

La chaîne de blocs ou « blockchain » en anglais est une technologie numérique innovante de stockage et de partage d'un registre de transactions au moyen d'un réseau pair-à-pair. Apparue en 2008 dans un article publié sous le pseudonyme de Satoshi Nakamoto, elle est utilisée depuis 2009 pour faire fonctionner ce qui en constitue l'exemple le plus emblématique : la cryptomonnaie Bitcoin, dont la capitalisation totale atteint aujourd'hui quelques 20 milliards de dollars, mais elle est également déclinée sous de nombreuses variantes moins connues.

Les promesses de la technologie sont fortes : celles d'un registre public partagé et sécurisé fonctionnant sans organe central de contrôle. Les blockchains sont peut-être ainsi promises à un avenir important dans le domaine bancaire (bitcoin), en finance, dans la gestion de contrats, dans les échanges énergétiques... En contrepoint, cette technologie présente un certain nombre d'inconvénients susceptibles de freiner son développement : consommation énergétique et volumes de stockage nécessaires importants, incertitude sur sa résilience, difficulté à faire évoluer ses règles de fonctionnement, complexité par rapport à des architectures traditionnelles faisant appel à un tiers de confiance... De plus, son cadre juridique, national ou international, est loin d'être figé.

Dès lors, je souhaiterais que vous mettiez en place un groupe de travail que vous présiderez destiné à se prononcer sur les enjeux liés au développement de cette technologie. Vous me rendrez vos conclusions pour la fin du mois d'octobre.

Ce groupe de travail devra faire un état des lieux critique du développement de cette technologie, des travaux de recherche et du tissu économique et entrepreneurial, en particulier le positionnement français dans les écosystèmes européen et mondial. Il devra se prononcer autant que possible sur les caractéristiques, potentiel et intérêt de cette technologie, sur les variantes existantes (recours à des chaînes privées notamment) et les améliorations envisageables, et sur la manière dont l'État pourrait accompagner son développement. Certaines questions pourront faire l'objet de travaux spécifiques par des sous-groupes, dont les rapports seront annexés à vos travaux.

Le groupe de travail que vous formerez comportera une diversité d'acteurs : universitaires, entrepreneurs et représentants des secteurs d'activité les plus concernés, représentants de la société civile et des administrations. Mes équipes se tiennent à votre disposition pour vous aider dans la mise en place de ce groupe de travail et dans son fonctionnement. Elles assureront la fonction de rapporteur des travaux. Votre interlocuteur sera Lionel Janin, adjoint au directeur du département développement durable et numérique.

Vous remerciant pour votre collaboration, je vous prie de croire, Madame le Professeur, à l'assurance de mes sentiments les meilleurs.

Bien à vous


Michel YAHIEL



ANNEXE 2

COMPOSITION DU GROUPE DE TRAVAIL

Présidente

Joëlle Toledano, professeur émérite d'économie (chaire Gouvernance et régulation, université Paris-Dauphine)

Rapporteur

Lionel Janin, expert Numérique, France Stratégie

Secrétaire

Sammy Bebane, chargé de mission, France Stratégie

Membres

Patrick Amarelis, Direction interministérielle du numérique et du système d'information et de communication (DINSIC)

Emmanuelle Anceaume, chargée de recherche, CNRS IRISA

Thierry Bedoin, Chief Digital Officer, Direction de la transformation digitale, Banque de France

Alain Bensoussan, avocat, Lexing Alain Bensoussan

Bruno Biais, professeur d'économie, École d'économie de Toulouse

Guillaume Buffet, président de U, Renaissance numérique

Richard Caetano, Directeur général et cofondateur, Stratumn

Philippe Calvez, R & D Project Manager, ENGIE

Alain Clot, président, France Fintech

Georgie Courtois, avocat à la cour, De Gaulle, Fleurance & Associés

Michel Dahan, directeur général et membre du directoire, Kreaxi

Jean-Michel Dalle, directeur, Agoranov

Jean-Pierre Dardayrol, membre du Conseil général de l'économie (CGE)

Primavera De Filippi, chercheuse au CERSA (CNRS-Paris 2) et chercheuse associée au Berkman Center for Internet & Society (université de Harvard)

Alexandre Eich Gozzi, expert blockchain, Sopra Steria Consulting
Pierre Entremont, principal, Otium Venture
Jacques Favier, secrétaire, association Le Cercle du coin
Nadia Filali, copilote de LaBChain, Caisse des dépôts et consignations
Clément Gasull, doctorant en sociologie, Orange Labs – Mines ParisTech
Florence G'sell, professeur de droit, université de Lorraine
Franck Guiader, directeur du pôle Fintech, Autorité des marchés financiers (AMF)
Laurent Henocque, fondateur & CEO, Keeex
Philippe Honigman, entrepreneur, U Change
Matthieu Hug, président, Tilkal
Henri Isaac, président, Renaissance numérique
Daniel Kaplan, fondateur, Imaginizing the Future
Éric Larchevêque, CEO, Ledger
Laurent Leloup, Président, France Blockteck
Anne-Hélène Le Trocquer, avocat à la cour, De Gaulle, Fleurance & Associés
Simon Marsol, directeur Secteur Public Excellence IT, Sopra Steria Consulting
Clément Martin-Saint-Léon, directeur des marchés, de la consommation et de la prospective, Arjel
Adam Ouorou, directeur du domaine de recherche « Confiance et Sécurité », Orange Labs Recherche
Romain Pigenel, directeur de programme, Maltem
Simon Polrot, cofondateur, directeur des opérations et du juridique, variabL.io
Loïc Poujol, Practice Manager Digital, Maltem
Alain Roset, conseiller auprès de la présidente de la branche numérique, La Poste
Xavier Simonin, Partner, Sopra Steria Consulting
Alexandre Stachtchenko, cofondateur, Blockchain France
François Stephan, directeur général adjoint en charge du développement et de l'international, Institut de recherche technologique, SystemX
Jacques Stern, cryptologue, Autorité de régulation des communications électroniques et des postes (ARCEP)
Adli Takkal Bataille, président, association Le Cercle du coin
Hubert de Vauplane, associé, Kramer Levin Naftalis & Frankel
Didier Warzée, expert Fintech, Autorité de contrôle prudentiel et de résolution
Cécile Wendling, directrice de la prospective, AXA



ANNEXE 3

LISTE DES RENCONTRES ET AUDITIONS

Cycle d'auditions Blockchains

Antoine Bargas, chargé de mission post-marché, AMF

Thierry Bedoin, Chief Digital Officer, Banque de France

Julien Béranger, consultant Blockchain

Sacha Bourgeois-Gironde, université de Paris 2/Lemma, Institut Jean-Nicod, ENS

Nabil Bouzerna, architecte Plateformes, SystemX

Richard Caetano, CEO et cofondateur

Philippe Calvez, R & D Project Manager, Engie

Domitille Dessertine, Policy Officer, Fintech Innovation & Competitiveness, AMF

Philippe Dewost, directeur adjoint, chargé de l'économie numérique, mission Programme d'investissements d'avenir, Caisse des dépôts et consignations

Nadia Filali, co-pilote LaBChain, Caisse des dépôts et consignations

Franck Guiader, directeur, Division FinTech, Innovation, Compétitivité, AMF

Nicolas Julia, Director of Business Operations, Stratumn

Odile Lakomski-Laguerre, université de Picardie-Jules-Verne

Éric Larchevêque, fondateur de Ledger, président de La Maison du Bitcoin

Xavier Laveyssière, consultant Blockchain & Régulation

David Manset, président-directeur général de Gnúbila, directeur de la recherche et de l'innovation d'Almerys

Louis Margot-Duclos, cofondateur de 97.network

Audrey Metzger, juriste, Banque de France

Pierre Noizat, cofondateur de Paymium

Alan Ouakrat, maître de conférences en sciences de l'information et de la communication, université Sorbonne Nouvelle, Paris 3

Jean-Michel Pailhon, Fintech Strategy Advisor

Pierre Paperon, entrepreneur, fondateur, SystemX

Simon Polrot, cofondateur VariabL, expert Blockchain

Pierre Porthaux, président-directeur général d'EmergenceLab, co-fondateur et président de Blockchain Solutions

Renaud Sirdey, directeur de recherche, Centre de recherche CEA Saclay

Didier Warzée, Fintech expert, Autorité de contrôle prudentiel et de résolution, Banque de France

Auditions du groupe de travail

Emmanuelle Anceaume, chargée de recherche CNRS au laboratoire IRISA

Laurent Bénichou, directeur R & D chez Axa

Vincent Danos, directeur de recherche au CNRS au département d'informatique de l'ENS, équipe Antique et membre du Centre de recherches interdisciplinaires (CRI)

Primavera De Filippi, chercheuse au CERSA (CNRS - université Paris 2) et chercheuse associée au Berkman Center for Internet & Society (Harvard)

Émilien Dutang, directeur général de Blockchain Partner

Auditions individuelles

Iskender Akhoune, CTO & Head of IT Unit, RaDiCo (rare disease cohorts)

Alexandra Barreau-Jouffroy, adjoint au bureau A de la Direction de la législation fiscale, ministères de l'Économie, des Finances, de l'Action et des Comptes publics

Benjamin Besnier, Lutte anti-blanchiment-financement du terrorisme, Direction générale du Trésor

Éric Bevillard, Technology Transfer Officer, CEA

Guillaume Bouyt, adjoint au bureau A de la Direction de la législation fiscale, ministères de l'Économie, des Finances, de l'Action et des Comptes publics

Christian Cachin, cryptographe et informaticien

Geoffroy Cailloux, chef du bureau Épargne et marché financier, Direction générale du Trésor

Vidal Chriqui, Chief Innovation Officer, Bitcoin and Blockchain Speaker, Syntec Numérique

Georges Gonthier, équipe SPECFUN du centre Inria Saclay – Île-de-France

Sébastien Griffon, directeur général, PlayItOpen

Thierry Grumiaux, délégué commission internationale, douane et logistique, FNTR (Fédération nationale des transports routiers)

Christoph Jentzsch, fondateur et CTO, Slock.it

Julien Leconte, directeur général, PlayitOpen

Bastien Llorca, sous-directeur du Contrôle fiscal, Direction générale des finances publiques, ministère de l'Économie et des Finances

Angélique Monneraye, chargée de mission Lutte contre la contrefaçon, Direction générale des entreprises, ministère de l'Économie et des Finances

Georges Nahon, CEO Orange Silicon Valley, President of Orange Institute, Orange Labs

Pierre Paperon, cofondateur, société Solid

Antoine Petit, président-directeur général, Inria

Wilfrid Pimenta de Miranda, Business Development Director, IOTA

Élisabeth Pons, adjointe au chef du Bureau A de la Direction de la législation fiscale, ministères de l'Économie, des Finances, de l'Action et des Comptes publics

Christophe Pourreau, directeur de la législation fiscale, Direction générale des finances publiques, ministères de l'Économie, des Finances, de l'Action et des Comptes publics

Hugo Rolland, Direction générale du Trésor

Stephan Tual, fondateur & COO Slock.it

Henri Verdier, directeur de la DINSIC, SGMAP

Marko Vukolić, membre du personnel de recherche, IBM Research Zurich



ANNEXE 4

APPLICATIONS DES BLOCKCHAINS AUX JEUX EN LIGNE

EXTRAIT D'UNE NOTE INTERNE DE L'ARJEL

L'Autorité de régulation des jeux en ligne (ARJEL) nous autorise à reproduire une note interne datée du 7 juillet 2017. Annoncée comme un « game changer », la technologie de la blockchain pourrait entraîner une série d'innovations dans l'industrie des jeux en ligne. Celle-ci se prépare à créer de nouveaux outils tels « les jeux à équité prouvée », fondés sur la blockchain. L'intérêt de l'industrie du jeu pour cette technologie est en soi un signe révélateur : on sait combien ce secteur a souvent été pionnier dans l'appropriation des innovations numériques.

1. Bitcoins et jeux en ligne

La législation en Europe

Concernant les activités de jeux en ligne en France, l'article 17 de la loi n° 2010-476 du 12 mai 2010 précise que « l'approvisionnement d'un compte joueur par son titulaire ne peut être réalisé qu'au moyen d'instruments de paiement mis à disposition par un prestataire de services de paiement établi dans un État membre de la Communauté européenne ou un État partie à l'accord sur l'Espace économique européen ayant conclu avec la France une convention contenant une clause d'assistance administrative en vue de lutter contre la fraude et l'évasion fiscales. Seuls peuvent être utilisés les instruments de paiement mentionnés au chapitre III du titre III du livre I^{er} du code monétaire et financier. »

Ainsi, en l'état actuel des textes, les opérateurs agréés en France ne pourraient pas proposer légalement à leurs joueurs d'approvisionner leurs comptes en Bitcoins directement. L'approvisionnement d'un compte par l'intermédiaire de Paymium (ou

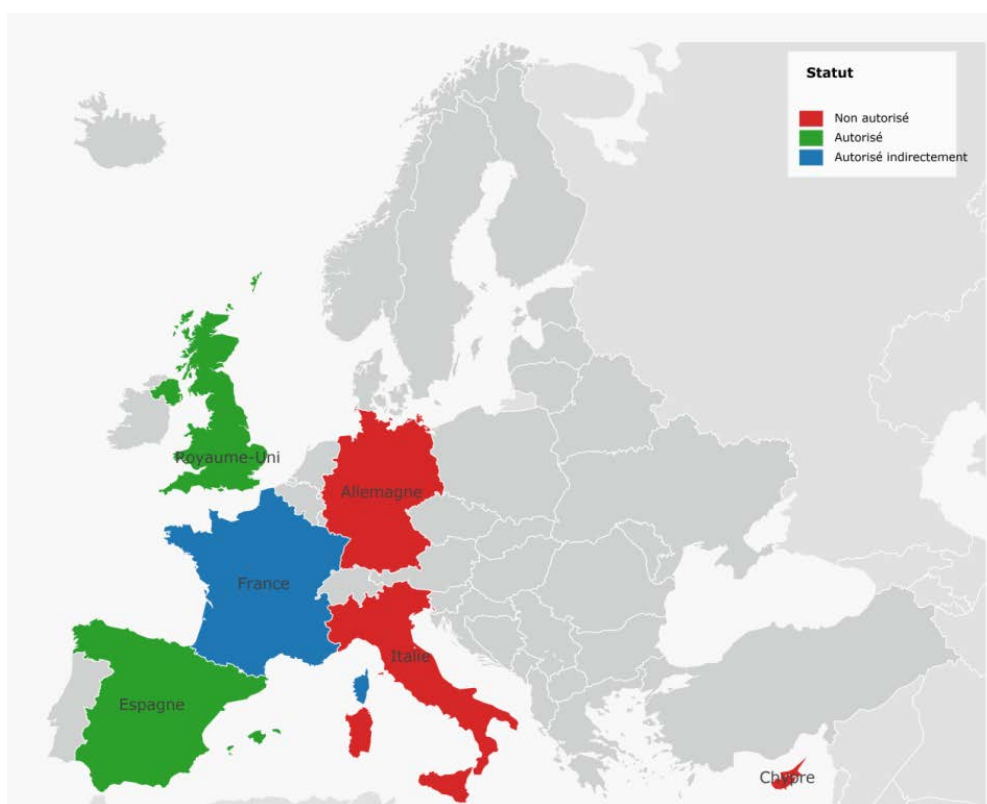
similaire) pourrait cependant être en accord avec la loi. Cette « banque Bitcoin » est, en effet, en conformité avec la législation européenne sur les services de paiement. Il n'y aurait également rien d'illégal à ce qu'un opérateur agréé distribue des Bitcoins à ses joueurs en ligne au titre de bonus ou de gains « en nature ».

Royaume-Uni – La Gambling Commission a, quant à elle, autorisé les opérateurs licenciés à accepter les monnaies digitales comme moyen de paiement.

Allemagne – L'Allemagne reconnaît le Bitcoin comme monnaie officielle depuis août 2013. Dans le cadre des jeux en ligne, notamment des problématiques de blanchiment d'argent, la loi stipule « que les joueurs doivent uniquement utiliser des moyens de paiement transparents pour alimenter leur compte ». Le Bitcoin n'est, a priori, pas considéré comme une monnaie transparente.

Italie – Comme en France, la devise autorisée sur les sites agréés en Italie est l'euro, mais certains prestataires de services de paiement proposent d'acheter des euros avec des bitcoins.

Figure 3 – Statut légal des paiements en Bitcoin dans les jeux en ligne en Europe



Source : Gisco - Eurostat

Espagne – L’Espagne a reconnu le Bitcoin comme monnaie en décembre 2014. Les opérateurs souhaitant proposer une offre en Bitcoin en Espagne devront en faire la demande auprès du régulateur espagnol et opérer sous agrément (note 2014).

Malte – Malte, après réflexion, a interdit l’utilisation des Bitcoins sur ses sites licenciés.

L’île de Man – L’île de Man a autorisé le dépôt d’argent en Bitcoin dans les casinos en ligne en mai 2016.

Chypre – L’utilisation du Bitcoin est interdite sur les sites des opérateurs de jeux en ligne licenciés.

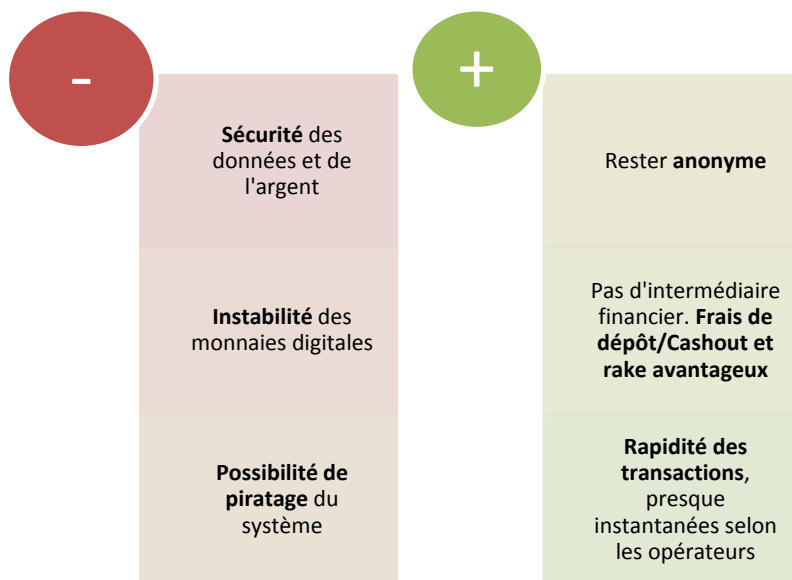
Accessibilité en France

Malgré l’interdiction d’accepter les monnaies digitales comme moyen de paiement, plusieurs casinos en ligne les proposant sont accessibles depuis la France. Certains opérateurs, à l’instar de 1Xbet, font partie des leaders du marché européen des casinos en ligne. Certains autres, comme Cloubet, ont choisi de se positionner en « *pure player* » et n’acceptent que les monnaies virtuelles.

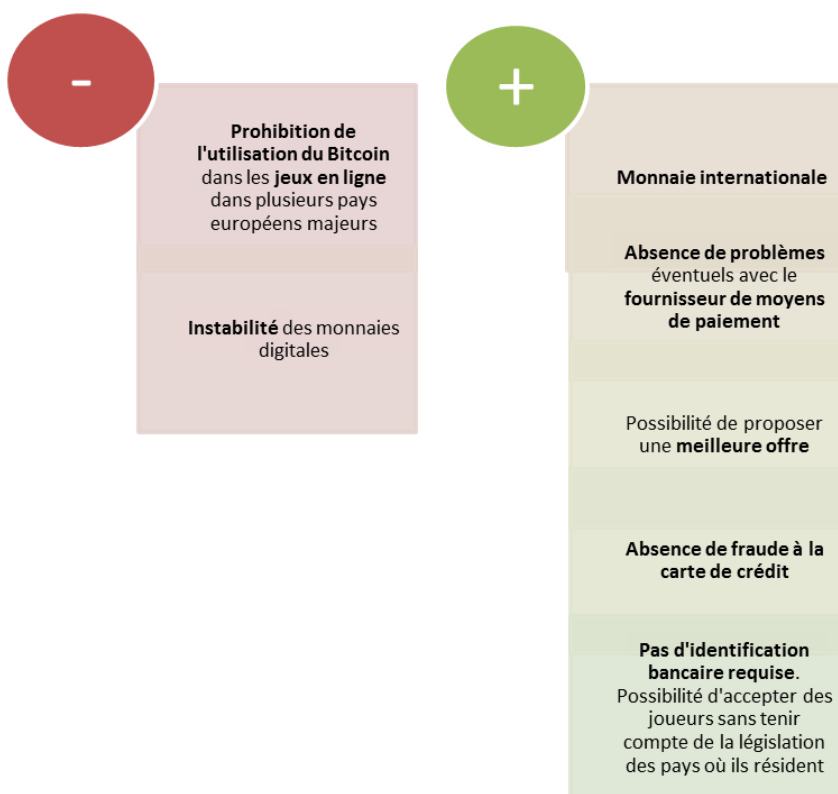
Tableau 1 – Exemples de casinos utilisant les Bitcoins accessibles en France

Site	Pays d'origine	Plateforme	« Pure player » monnaie virtuelle	Casino	Paris sportifs	Poker
1Xbet	Curaçao	nd	☐	☐	☐	☐
Bitstarz.com	Malte	isoftbet	☐	☐	☐	☐
Onlinecasino.ac	Costa Rica	Betsoft	☐	☐	☐	☐
Playamo.com	Curaçao	SoftSwiss	☐	☐	☐	☐
Cloubet.com	Montenegro	nd	☐	☐	☐	☐
Sportsbet.io	Curaçao	nd	☐	☐	☐	☐
NitrogenSports.eu	Costa Rica	nd	☐	☐	☐	☐
Betcoin.ag	nd	Betsoft	☐	☐	☐	☐

Avantages/désavantages des monnaies virtuelles pour les joueurs



Avantages/désavantages des monnaies virtuelles pour les opérateurs



Avantages/risques pour les régulateurs

Du point de vue des pouvoirs publics, les transactions en Bitcoins présentent aussi l'inconvénient de pouvoir être totalement anonymes si les vendeurs et acheteurs ne souhaitent pas dévoiler leurs identités respectives. Les flux sont publics et tracent les adresses d'émission et de réception des Bitcoins mais les utilisateurs pouvant créer des adresses Bitcoin multiples, celles-ci ne constituent pas un moyen d'identification ou d'authentification. Le site bitcoin.fr précise ainsi que « les utilisateurs de Bitcoins peuvent créer autant d'adresses qu'ils le veulent et, en pratique, sont encouragés à en générer une nouvelle pour chaque transaction s'ils veulent préserver une certaine confidentialité »¹.

De ce fait, et toujours de l'aveu même des gestionnaires du système, Bitcoin favorise le blanchiment et l'évasion fiscale².

Ainsi, en octobre 2013, le site Internet *Silk Road* a été fermé par les autorités américaines et son responsable arrêté, après qu'elles ont découvert que le site en question était devenu une plaque tournante de la drogue où les vendeurs et acheteurs du monde entier s'échangeaient des substances illicites en profitant de l'anonymat des transactions en Bitcoins.

Le 5 décembre 2013, la Banque de France a – à son tour – mis en garde les utilisateurs de Bitcoins des risques encourus en termes de blanchiment de capitaux et a rappelé que « l'activité de conversion contre monnaie ayant cours légal offerte par les plates-formes internet [...] doit s'analyser [...] comme un *service de paiement nécessitant un agrément* de prestataire de service de paiement »³, invitant ainsi les sites proposant l'achat ou la vente de Bitcoins à se manifester auprès de l'Autorité de contrôle prudentiel, en France, ou les services compétents à l'étranger.

L'instabilité des monnaies digitales pose aussi un problème aux régulateurs, en termes d'incitations données aux joueurs. Favoriser l'utilisation de Bitcoin, tout en connaissant la forte volatilité de cette monnaie peut, en effet, être contraire aux objectifs de protection des consommateurs de l'ARJEL.

¹ <http://www.bitcoin.fr/pages/Fonctionnement#main>.

² <http://www.bitcoin.fr/pages/Vices-et-vertus#main>.

³ Banque de France – Focus – n° 10 – 5 décembre 2013.

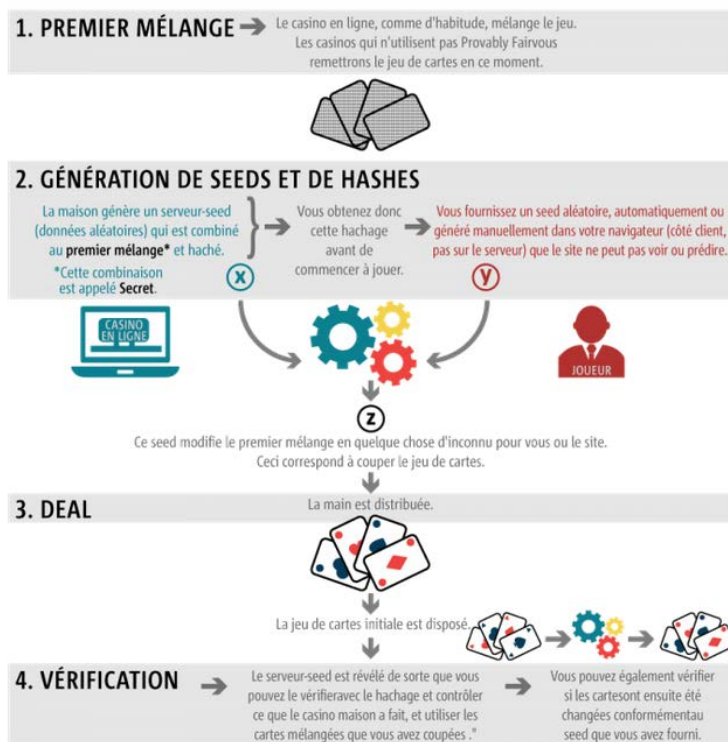
2. Utilisation de la technologie Blockchain dans les casinos en ligne

Provably fair games

Certains opérateurs de jeux en ligne utilisent déjà la blockchain pour proposer des jeux à équité prouvée. L'idée est de permettre aux utilisateurs de vérifier que les résultats du jeu sont réellement aléatoires, notamment dans le cas de parties de poker ou de jeux de casino.

En pratique, le résultat d'un jeu est déterminé par une combinaison de facteurs (*seeds*) à travers un algorithme public (SHA256). Ces facteurs proviennent à la fois du serveur de jeu (opérateur) et du client (joueur). Chaque combinaison de facteurs génère un résultat unique, de sorte qu'aucune des deux parties n'ait de possibilité de le manipuler. Une fois les résultats dévoilés, le joueur a accès au *seed* de l'opérateur. Il peut alors vérifier si le résultat du jeu dévoilé correspond bien à la combinaison de facteurs (serveur + client) utilisée pour la partie à l'aide d'un logiciel de décryptage. Certains casinos en ligne, à l'instar de PrimeDice, proposent même un outil de vérification intégré. De nombreux encodeurs en ligne tels que quickhash.com offrent également aux joueurs la possibilité de vérifier l'équité d'un jeu à travers l'algorithme SHA256.

Figure 4 – Fonctionnement des jeux à équité prouvée



Source : <https://www.casinosbitcoin.fr/provably-fair/>

Bitlotto est un des premiers sites à avoir proposé des « provably fair games ». Maintenant fermé, il utilisait les identifiants spécifiques à chaque transaction Bitcoin pour déterminer un numéro de ticket de loterie. Les chiffres gagnants étaient ensuite générés en s'appuyant sur le tirage de la loterie gouvernementale. Les joueurs pouvaient ainsi vérifier que les résultats de jeu n'étaient pas manipulés par l'opérateur. Certains sites proposant des « provably fair games » sont accessibles en France, à l'instar de Playalamo ou PrimeDice.

Tableau 2 – Exemples de sites proposant une offre de jeux en équité prouvée accessible en France

Site	Fournisseurs de jeux	« Pure player » Monnaie virtuelle
Goldenstar-casino19.com	Amatic, BetSoft, NetEnt, Ezugi, SoftSwiss, Microgaming, Pragmatic Play, Endorphina	☐
Playamo	SoftSwiss	☐
PrimeDice	-	☐
games.bitcoin.com	Propriétaire	☐

Smart contracts

Certains autres opérateurs ont décidé de construire leurs logiciels autour de la technologie blockchain. L'architecture de ces derniers s'articule autour des *smart contracts*.

- *Smart contracts* : éléments de compréhension

Le site officiel bitcoin.fr définit les smart contracts comme « un transfert de valeurs automatisé fondé sur des conditions mutuellement convenues, qui peut avantageusement s'exécuter sur la blockchain Bitcoin ».

Les *smart contracts*, et plus généralement la technologie Blockchain, sont conçus pour éliminer le besoin de confiance dans les interactions entre différents agents. Imaginons un contrat entre deux personnes. A souhaite rémunérer B pour l'exécution d'une prestation. Les termes de cet engagement sont inscrits sur la blockchain par l'intermédiaire d'un *smart contract*. Dans le même temps, l'argent de A est mis en gage sur la blockchain. Une fois les conditions réunies (exécution de la prestation), l'argent de A est envoyé automatiquement sur le compte de B. Si les termes du

contrat sont directement liés à la blockchain, ceux-ci s'exécutent automatiquement, sans l'intervention d'un tiers. Si les conditions sont extérieures à la blockchain, les contractants doivent faire appel à un tiers (personne de confiance, base de données), appelé « oracle », pour inscrire les informations nécessaires dans le système. Dans le cadre de paris sportifs, les utilisateurs peuvent, par exemple, adosser leur contrat à une base de données répertoriant les résultats.

Les *smart contracts* pourraient aussi s'appliquer au paiement automatique d'une livraison. Plusieurs projets impliquant ces contrats sont actuellement en cours. Selon Bitcoin.fr, des développeurs costaricains travaillent sur un projet de création de cadastre en utilisant ces nouveaux contrats.

La start-up française WeKeep cherche, quant à elle, à développer un système d'assurance sans tiers.

Selon Nick Szabo, un informaticien et cryptographe américain, les *smart contracts* réduiraient considérablement les contentieux. Les théoriciens de la blockchain parlent même de « notariation » des contrats. Ceux-ci sont rédigés, suivis et mis en œuvre par le biais d'un protocole audité par les parties prenantes elles-mêmes.

Les deux principaux projets qui développent des systèmes construits autour des *smart contracts* sont Ethereum et Codius. Toujours en cours de développement, ces plateformes ont pour ambition de devenir le système sur lequel s'appuieront les futures applications « *smart contracts* ».

- *Smart contracts* et jeux en ligne

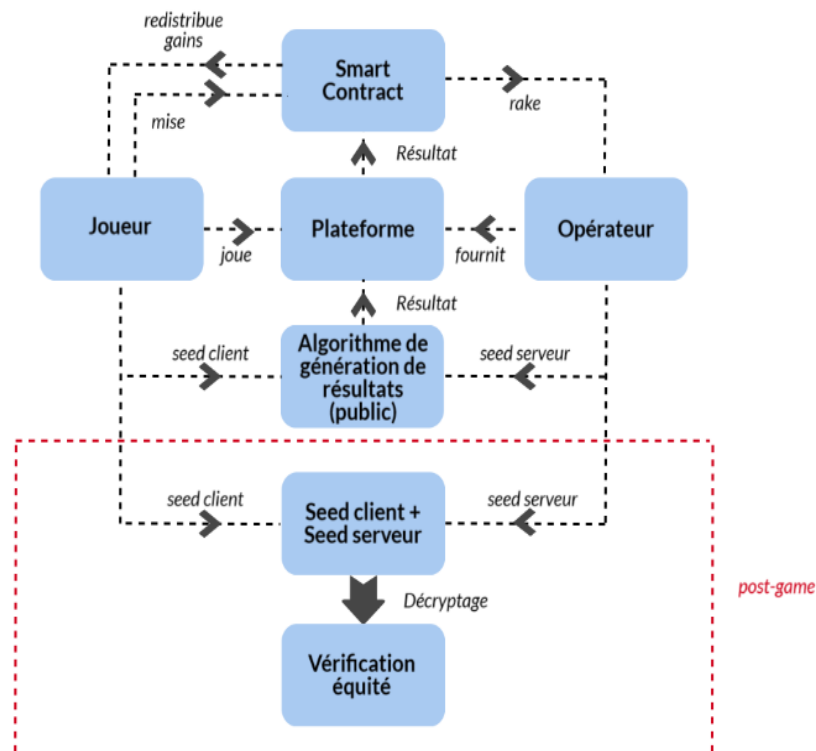
Constatant que les joueurs étaient réticents à faire confiance aux casinos en ligne, plusieurs entreprises ont commencé à développer des applications s'appuyant sur les *smart contracts* d'Ethereum. Ces plateformes cherchent à convertir la totalité de la chaîne de valeur des sites de jeux en ligne en système décentralisé afin d'éliminer la notion de confiance dans l'industrie des jeux en ligne. L'objectif est de minimiser l'intervention humaine en automatisant et décentralisant le plus grand nombre d'aspects possibles, de sorte qu'aucune partie prenante ou tierce n'ait de contrôle sur le processus.

➤ **EtherPoker**

Le projet EtherPoker, de l'entreprise Consensys utilise les *smart contracts* pour mettre en place une plateforme de poker décentralisée de pairs à pairs. Les deux principales caractéristiques de ce projet :

- un joueur gardera le contrôle de ses fonds Ether en permanence, sauf au moment du jeu (pas de dépôt). Au cours du jeu, les enjeux sont placés sur un *smart contract* Ethereum qui redistribue les gains automatiquement à la fin de la partie.
- la plateforme fournira des preuves d'équité, sous forme d'un code *open source*, de la même manière que les *provably games* classiques.

Figure 5 – Fonctionnement EtherPoker



➤ Les projets DAO (Decentralized autonomous organizations)

Les projets DAO ont pour ambition de convertir toute la chaîne de valeur d'un casino en ligne sous forme de *smart contracts*. Le système n'existe et les joueurs n'interagissent que sur la blockchain. Différents projets, tels que DAO.Casino ou Pokereum, ont vu le jour récemment. Ils s'appuient sur les 3 types d'acteurs classiques : les développeurs, les opérateurs de plateformes et les joueurs. Une multitude de *smart contracts* est mise en place pour définir tous les aspects de l'industrie du jeu en ligne, de développement à la redistribution des gains. Aucun participant ou tiers n'a de contrôle sur les résultats et les gains. Les développeurs sont par exemple récompensés automatiquement en fonction de l'utilisation de leurs jeux. Les joueurs reçoivent leurs gains immédiatement après avoir gagné. Ils n'ont

pas besoin d'effectuer de dépôts. N'importe qui, avec les compétences et ressources nécessaires, peut opérer une plateforme et prendre une commission s'il le souhaite. La plateforme n'a pas de contrôle sur les jeux, si ce n'est qu'elle sélectionne ceux qu'elle souhaite diffuser. Le programme et le code de la plateforme sont publics, de sorte que les participants peuvent vérifier si les processus sont équitables. DAO.Casino a notamment prévu de proposer des outils qui permettent aux joueurs de vérifier automatiquement l'équité des jeux.

3. À retenir

- La blockchain est une technologie de stockage et d'échange d'informations fonctionnant sans organe de contrôle. Actuellement en plein essor, l'application la plus célèbre de cette technologie est la monnaie virtuelle Bitcoin.
- La blockchain est parfaitement adaptée au transfert de monnaie. L'industrie du e-commerce s'y intéresse donc de près. Plusieurs sites majeurs accessibles en France proposent déjà une option « paiement en Bitcoin » : Showroomprivé.com, Expedia.com, Isilines.fr et Airbaltic.com. Les transferts se font par l'intermédiaire de prestataire de services de paiement ayant obtenu l'agrément ACPR, à l'instar de Paymium.
- La majorité des pays européens n'autorisent pas le paiement en Bitcoin dans l'industrie des jeux en ligne. Le Royaume-Uni, l'Espagne et l'île de Man ont cependant permis à leurs sites licenciés d'accepter les monnaies digitales comme moyen de paiement.
- La loi française autorise, *a priori*, le dépôt de Bitcoin, par l'intermédiaire de prestataires agréés (Paymium ou similaire) sur les sites de jeux en ligne agréés par l'ARJEL.
- Plusieurs sites de jeux en ligne illégaux (casino, poker, paris sportifs) autorisant le dépôt en monnaie digitale, dont 1X Bet, sont accessibles depuis la France. Certains ont même choisi d'accepter uniquement les Bitcoins comme moyen de paiement (Cloubet.com, Sportsbet.io, NitrogenSports.eu).
- Le jeu en Bitcoin présente plusieurs avantages pour les joueurs : anonymat, rapidité des transactions et frais de jeu minimaux. L'instabilité des monnaies digitales et les possibilités de piratage du système sont cependant des risques significatifs pour ces joueurs.

- Les opérateurs peuvent avoir intérêt à accepter les monnaies virtuelles. L'absence d'intermédiaires financiers leur permet de proposer une meilleure offre et de ne pas avoir de problème avec les fournisseurs de moyens de paiement. Tout comme les joueurs, l'instabilité du Bitcoin est une source de risque significative pour ces agents.
- Le relatif anonymat dont jouissent les joueurs en monnaie virtuelle représente un inconvénient pour les régulateurs, notamment dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme.
- Outre le paiement en monnaie virtuelle, l'industrie des jeux en ligne a vu apparaître une série d'innovations reposant sur la blockchain.
- Certains opérateurs proposent des « jeux à équité prouvée ». Ils utilisent la blockchain, notamment des algorithmes en *open source*, pour prouver en temps réel que les résultats des jeux sont véritablement aléatoires. Les joueurs peuvent ainsi vérifier par eux-mêmes que les résultats ne sont pas manipulés. Cette « auto-certification » pourrait signer la fin de l'activité des certificateurs de jeux traditionnels.
- Les projets DAO (*Decentralized autonomous organizations*), qui s'appuient sur les *smart contracts*, trouvent aussi une application dans les jeux en ligne. Ils ont pour ambition de convertir toute la chaîne de valeur des jeux en ligne, du développement à la redistribution des gains, sous forme de *smart contracts*. Le système n'existe et les joueurs n'interagissent que sur la blockchain. Les deux principaux projets de ce type sont DAO.Casino et Pokereum.



Directeur de la publication

Gilles de Margerie, commissaire général

Directeur de la rédaction

Fabrice Lenglard, commissaire général adjoint

Rédacteur en chef

Olivier de Broca

Contact presse

Jean-Michel Roullé, directeur du service Édition/Communication/Événements

01 42 75 61 37, jean-michel.roulle@strategie.gouv.fr

RETROUVEZ
LES DERNIÈRES ACTUALITÉS
DE FRANCE STRATÉGIE SUR :



www.strategie.gouv.fr



[francestrategie](https://www.facebook.com/francestrategie)



[@Strategie_Gouv](https://twitter.com/Strategie_Gouv)

Ce rapport est publié sous la responsabilité éditoriale du commissaire général de France Stratégie. Les opinions exprimées engagent leurs auteurs et n'ont pas vocation à refléter la position du gouvernement.



FRANCE STRATÉGIE



France Stratégie est un organisme d'études et de prospective, d'évaluation des politiques publiques et de propositions placé auprès du Premier ministre. Lieu de débat et de concertation, France Stratégie s'attache à dialoguer avec les partenaires sociaux et la société civile pour enrichir ses analyses et affiner ses propositions. Elle donne à ses travaux une perspective européenne et internationale et prend en compte leur dimension territoriale.