# La blockchain et l'intermédiation financière[1]

Marianne Verdier[2]

20 décembre 2017

Résumé

La blockchain est une technologie permettant d'effectuer et d'enregistrer des transactions ordonnées sous format numérique dans un réseau décentralisé sans avoir recours à un tiers de confiance. Les échanges sont sécurisés par l'usage d'algorithmes de cryptographie. Dans cet article, nous étudions l'impact de cette innovation sur l'activité des intermédiaires financiers. Nous montrons que la blockchain est susceptible de réduire les coûts associés à l'intermédiation financière, entraînant une évolution du rôle du tiers de confiance pour les transactions financières. Cependant, la réglementation doit encadrer son développement afin de sécuriser les échanges et de favoriser son adoption.

JEL codes: G21, G23, G01, O33, D40

Mots-clés: Blockchain, banques, Fintech, intermédiation financière, cybermonnaies, bitcoin, réglementation financière, ICO, smart contracts.

[1] Je remercie Jean-Michel Pailhon pour ses commentaires et suggestions.
[2] CRED, Université Paris 2 Panthéon Assas, CERNA, Ecole des Mines de Paris.

[2] CRED, Université Paris 2 Panthéon Assas, CERNA, Ecole des Mines de Paris.

[3] Pour des contributions très complètes en français sur les applications de la blockchain en finance, voir Collomb et Sok (2016) et le rapport de Paris Europlace (2017). Pour une synthèse sur les enjeux

## 1- Introduction

Dans le roman de science fiction « Fahrenheit 451 » de Ray Bradbury, un Etat dictatorial a décidé de brûler tous les livres que les citoyens détiennent chez eux. Ce projet fou est d'autant plus difficile à réaliser que les livres peuvent être copiés et dispersés dans les différentes maisons des citoyens : la décentralisation de l'information rend la censure plus coûteuse. Si Ray Bradbury avait pu concevoir l'existence d'un dispositif comme la blockchain, permettant d'enregistrer de l'information de façon immuable, sécurisée et décentralisée, il se serait peut-être moins inquiété du pouvoir de l'Etat sur la connaissance. L'existence d'une telle technologie pourrait-elle remettre en cause le pouvoir des intermédiaires financiers sur l'information financière? La blockchain peut-elle réduire les coûts de l'intermédiation financière? Cette innovation entraîne-t-elle l'apparition de nouveaux risques? Nous tentons de répondre à ces questions dans cet article.[3]

La technologie blockchain permet d'effectuer et d'enregistrer des transactions sous format numérique sans avoir nécessairement recours à un tiers de confiance. L'information est inscrite dans des blocs de transactions ordonnés chronologiquement (la chaîne de blocs), chaque bloc étant relié par son identifiant au bloc précédent. Une blockchain est une catégorie de « registre distribué » (DLT), pour faire référence au fait que les copies du registre sont disponibles dans chacun des nœuds du réseau.[4] Il s'agit d'une application décentralisée (dApp) dont le protocole définit la façon dont le registre est détenu, mis à jour et surveillé par l'ensemble des participants. Deux membres du réseau peuvent ainsi effectuer des transactions « en pair à pair » sans intervention d'une autorité centrale.[5] Les autres membres deviennent alors témoins de la transaction et se mettent d'accord sur le fait que celle-ci a bien été effectuée. Quand un consensus entre les participants est atteint, la transaction peut être enregistrée dans chacun des nœuds du réseau. Les participants sont encouragés à participer aux opérations communes de vérification et de mise à jour du registre par des mécanismes d'incitation économiques définis dans le protocole. Par ailleurs, les transactions sont sécurisées par l'usage d'algorithmes de cryptographie.

Le premier usage de la blockchain est apparu en 2009 avec la mise en service d'une cybermonnaie appelée bitcoin.[6] Pour la première fois, un article signé sous le pseudonyme de Satoshi Nakamoto propose un protocole permettant d'enregistrer des transactions électroniques de façon décentralisée, sécurisée et transparente, rendant impossible toute double dépense des bitcoins. Depuis la création du bitcoin, différentes sortes de blockchains se sont développées.[7] Elles se distinguent par le degré d'ouverture

---

[3] Pour des contributions très complètes en français sur les applications de la blockchain en finance, voir Collomb et Sok (2016) et le rapport de Paris Europlace (2017). Pour une synthèse sur les enjeux économiques de la blockchain, voir Waelbroeck (2017) et Gans et Catalini (2017).

[4] Le sigle DLT fait référence à l'expression « Distributed Ledger Technology » en anglais. Tous les registres distribués ne sont pas forcément structurés en chaînes de blocs.

[5] Selon Davidson et al. (2016), les premiers registres comptables sont apparus à Venise au quinzième siècle. Les registres ont été digitalisés au vingtième siècle et sont restés centralisés jusqu'à l'apparition de la blockchain en 2008.

[6] L'article décrivant le protocole Bitcoin a été publié en 2008 sous le pseudonyme de Sakamoto. Le premier bloc de transactions en bitcoins a été créé en janvier 2009.

[7] Par extension, une blockchain particulière désigne un réseau et son protocole de fonctionnement.

du réseau, la taille des blocs ajoutés, la nature et la transparence de l'information diffusée, les méthodes utilisées pour parvenir à un consensus et valider les transactions, les modes de consultation du registre, les modes de gouvernance pour mettre à jour le protocole.

Les applications de la blockchain sont nombreuses.[8] En finance, la technologie peut être utilisée pour réaliser des échanges de cybermonnaies[9], de titres financiers, enregistrer des droits de vote associés à des actions, lever des fonds par une ICO (« Initial Coin Offering ») en créant des titres de participation associés à des jetons (« tokens ») échangeables contre des cybermonnaies, programmer l'exécution de contrats intelligents (« smart contracts »). D'autres usages se sont également développés en dehors du système financier, comme pour l'archivage des registres cadastraux au Ghana, l'enregistrement d'actes notariés en Estonie ou le stockage de données privées relatives à la santé (e.g., Bithealth).

Dans un système financier, les banques et les institutions financières assument le rôle de tiers de confiance pour les transactions financières (paiements, échanges de titres financiers, enregistrements de garanties). Elles créent de la valeur sur les marchés en collectant de l'information de façon sécurisée, confidentielle et organisée.[10] En contrepartie, elles disposent d'un pouvoir de marché et d'un accès privilégié aux données de leurs clients. Elles ont aussi la capacité de restreindre l'accès de certains participants au système financier. La blockchain va-t-elle faire évoluer le rôle du tiers de confiance assumé par les banques et les institutions financières? Les coûts de l'intermédiation financière vont-ils être réduits? Quels sont les risques associés à la blockchain et comment les réguler ?

Selon Harvey (2016), l'usage de la cryptographie pour sécuriser les échanges financiers sans tiers de confiance va donner naissance à un nouveau champ de recherche, la « cryptofinance ».[11] Cette discipline s'intéresse notamment aux mécanismes permettant de conclure des contrats financiers sans tiers de confiance et à l'impact de la technologie sur l'organisation des systèmes financiers. En effet, la blockchain remet en cause le pouvoir des intermédiaires sur l'information financière, rendant leurs activités contestables par de nouveaux entrants (Wright et De Filippi, 2015, Gans et Catalini, 2017). Les services innovants offerts par les start-ups fintechs pourraient réduire les coûts de l'intermédiation financière, restés relativement stables depuis une centaine d'années en Europe et aux Etats-Unis (Philippon, 2016).

Dans la première partie, nous présentons les principales évolutions de la technologie blockchain et ses applications dans le secteur financier. Dans la seconde partie, nous étudions les mécanismes permettant de créer la confiance dans une blockchain. Dans la troisième partie, nous étudions l'impact de la blockchain sur les coûts de

[8] Il s'agit d'une technologie générique au sens de Bresnahan et Trajtenberg (1995), pouvant être utilisée dans de nombreux secteurs d'activités (voir Buterin, 2015).
[9] On rencontre également le terme « cryptomonnaie », traduction française du mot « cryptocurrencies » en anglais. Le journal officiel recommande l'usage du terme « cybermonnaie ».
[10] Il existe une vaste littérature tentant de mesurer la valeur informationnelle associée à l'activité des banques (voir Freixas et Rochet, 2008, chapitre 2).
[11] Voir aussi Babbitt et Dietz (2015) pour une définition de la cryptoéconomie.

l'intermédiation financière. Enfin, dans la quatrième partie, nous présentons les questions de réglementation associées au déploiement de cette technologie.

## 2- La blockchain et ses applications en finance

En finance, la blockchain peut être utilisée pour réaliser des transferts de cybermonnaies, enregistrer des droits de propriété, des échanges de titres financiers, programmer l'exécution de contrats financiers et lever des fonds en cybermonnaies.

*Transférer de l'argent grâce à une blockchain : du bitcoin aux cybermonnaies*

Les premiers développements de la technologie dite « blockchain 1.0 » concernent le Bitcoin et les échanges de cybermonnaies.[12] Le Bitcoin est un protocole permettant aux agents d'échanger des unités de compte sur une blockchain sans tiers de confiance. Le principe consiste à enregistrer dans le registre les droits de propriété des agents sur des unités de compte non dépensées.[13] Si Anna (pseudonyme) souhaite transférer des bitcoins à Tom (pseudonyme), l'ensemble du réseau doit pouvoir vérifier qu'elle ne les a pas dépensé avant, puis enregistrer le changement de propriétaire. Cet échange peut se réaliser de façon simple en utilisant un système de clés codées par des algorithmes de cryptographie. Anna doit disposer d'une clé privée (connue d'elle seule), d'une clé publique (qu'il est possible de diffuser à l'ensemble du réseau, créée à partir de la clé privée) et d'une adresse bitcoin (créée à partir de sa clé publique).[14] La clé privée lui donne le pouvoir de donner, de vendre, ou d'utiliser en garantie les bitcoins qui lui sont associés. Anna initie une transaction en envoyant au réseau un message chiffré avec sa clé privée, indiquant l'adresse du destinataire des bitcoins, le montant des bitcoins à transférer et sa clé publique. La clé publique sert à déchiffrer le message d'Anna. Elle permet à l'ensemble du réseau de vérifier qu'Anna n'a pas déjà dépensé les unités utilisées pour payer Tom (problème de la double dépense). L'information étant codée de façon unique au niveau d'une transaction, il n'est pas nécessaire pour cela de vérifier l'identité d'Anna (anonymat). Une fois la transaction validée, le réseau enregistre simplement le transfert de propriété.[15] Tom pourra ainsi dépenser les bitcoins reçus d'Anna en les envoyant au destinataire de son choix. Ultérieurement, nous expliquerons plus précisément comment la transaction peut être validée sans tiers de confiance dans un réseau décentralisé.

[12] Noter que le nom du protocole Bitcoin s'écrit avec un B majuscule tandis que le nom de la cybermonnaie bitcoin s'écrit avec un b minuscule. Le bitcoin est l'une des cybermonnaies associées au protocole Bitcoin. Pour une revue de la littérature sur le Bitcoin, voir Böhme et al. (2015), Halaburda et Sarvary (2016).

[13] L'état du système à un instant T est caractérisé par une collection d'UTXO, Unspent Transaction Output, soit des unités de transactions non dépensées.

[14] L'algorithme ECDSA ("Elliptic Curve Digital Signature Algorithm") permet de générer une clé privée, une clé publique à partir de la clé privée et une adresse bitcoin à partir d'une clé publique. L'usage d'une paire de clés privée et publique permet de chiffrer et de déchiffrer un message selon un principe de cryptographie asymétrique. Actuellement, par exemple (et pas uniquement), il est possible de générer des clés sur les sites des portefeuilles de bitcoins.

[15] Notons que le registre garde trace de tous les transferts mais pas des soldes comme dans les comptes bancaires traditionnels. Il existe également des solutions « multi-signatures » permettant de demander plusieurs clés potentiellement détenus par différents usagers pour réaliser une transaction.

Le code source du Bitcoin étant ouvert, il peut être utilisé librement, copié et retravaillé. Les modifications apportées à la version initiale ont ainsi abouti à la création de cybermonnaies alternatives, appelées les « altcoins » (e.g., Litecoin en 2011, Peercoin en 2012). Ces dernières peuvent différer des bitcoins par la quantité de monnaie émise, leur système de validation des transactions ou la taille des blocs enregistrés.[16] Un marché de concurrence entre cybermonnaies s'est développé (Gans et Halaburda, 2014), marquant la coexistence de différents standards associés au protocole Bitcoin pour réaliser des transferts de cybermonnaies. Au 27 novembre 2017, le bitcoin était valorisé à 162 milliards de dollars, l'ensemble des cybermonnaies étant valorisé à 302 milliards de dollars.[17] L'évolution du cours de change des cybermonnaies n'est cependant pas corrélée à leur diffusion. En effet, une étude réalisée par Schuh et Shy (2016) aux Etats-Unis montre que moins de 1,5% des consommateurs ont utilisé une monnaie virtuelle.

*Enregistrer la propriété sur la blockchain : altchains et colored coins*

Les usages de la blockchain se sont étendus au-delà des transferts de cybermonnaies. La technologie permet en effet d'enregistrer des transferts de propriété et de créer des méthodes pour aboutir à un consensus entre les participants d'un réseau sur l'état du système sans autorité centrale. Il est ainsi possible d'ajouter des couches d'instructions au protocole (les « altchains ») pour créer des algorithmes de consensus spécifiques, des systèmes d'enregistrement de noms, de titres de propriété et d'autres applications (« blockchain 2.0 »).[18]

Le protocole a été notamment modifié pour pouvoir enregistrer des transferts d'actifs digitaux appelés « colored coins ». Le principe consiste à associer des données supplémentaires aux unités de compte d'une blockchain (e.g., les bitcoins) pour les colorer d'un attribut, comme un mode d'émission, le fait de pouvoir les subdiviser, les agréger ou de leur associer le versement de dividendes. Une colored coin peut être imaginée comme un billet de banque tamponné, pouvant servir à la fois d'unité de compte et de titre représentant un actif (voiture, maison, titre financier, métaux précieux comme l'or). Les colored coins peuvent être achetées, vendues ou même être décolorées en leur retirant leur attribut spécial et rachetées à leur valeur faciale. Le transfert de propriété d'une colored coin peut donc représenter l'échange de n'importe quel actif, et plus particulièrement de titres financiers. La blockchain permet la création d'un système de règlement-livraison intégré, puisqu'il est possible de garder trace sur le même registre des échanges d'actifs et des unités de compte utilisées pour les régler. Le Nasdaq utilise déjà un système de colored coins avec le protocole Open Assets pour enregistrer des échanges de titres. BNP Paribas et la fintech SmartAngels ont également développé une blockchain pour enregistrer des échanges d'actions d'entreprises non cotées. [19]

[16] Pour plus de détail, voir Halaburda et Sarvary (2015).

[17] Source : coinmarketcap.com.

[18] Les altchains utilisent les briques élémentaires du protocole Bitcoin, avec parfois une autre cybermonnaie ou des jetons comme mécanisme de paiement mais n'ont pas pour objectif d'être une cybermonnaie. Par exemple, Namecoin utilise le protocole Bitcoin pour créer des noms de domaines en « .bit » décentralisés et ne pouvant être censurés par une autorité centrale, contrairement au Domain Name System.

[19] Le consortium R3 réunissant plus d'une quarantaine banques cherche actuellement à développer des solutions communes d'échanges de titres financiers. Par exemple, la blockchain Corda est utilisée dans le cadre d'un projet pilote pour échanger des obligations. On peut citer aussi les sociétés Chain ou Digital

*Programmer des contrats sur la blockchain : l'essor des « smart contracts »*

Enfin, la technologie blockchain a évolué autour de la possibilité d'associer des contrats intelligents ou « smart contracts » au registre de transactions. Un smart contract est un programme autonome, codé sur la blockchain, qui exécute automatiquement, tout ou partie d'un contrat sans intervention humaine. Dès lors qu'une condition préprogrammée du contrat intelligent est vérifiée, la clause contractuelle lui correspondant est automatiquement réalisée.[20] Apparu sur le marché en 2013, le protocole Ethereum est spécialement conçu pour programmer des contrats sur la blockchain de façon efficace.[21] Les smart contracts pourraient aboutir à la création de nouveaux produits financiers et de systèmes de gouvernance automatisés. Ils sont déjà utilisés dans le domaine des assurances. Par exemple, la compagnie Axa a développé la plateforme d'assurance fizzy pour indemniser automatiquement les passagers sur les retards des vols transatlantiques.[22]

*Financer un projet avec la blockchain : les Initial Coin Offerings*

Sur le modèle des introductions en bourse (IPO), la technologie blockchain peut aussi être utilisée pour lever des fonds dans le cadre des Initial Coin Offerings (ICOs). Ces opérations donnent lieu à une émission de jetons, les « tokens », achetés avec des cybermonnaies. En principe, la levée de fonds est réalisée grâce à la technologie blockchain sans intermédiaire financier. Les projets concernent le développement d'applications autour de la technologie blockchain ou la création de fonds d'investissement non régulés. Par exemple, le projet Master-Coin a levé plus de 5000 bitcoins en 2013 grâce à une ICO pour créer des fonctionnalités supplémentaires sur le protocole Bitcoin. Selon Gans et Catalini (2017), les ICOs constituent un moyen innovant pour attirer des talents, des liquidités et des idées autour d'un projet, sans tiers de confiance. La valeur apportée par les ICOs est liée à la mise en réseau des participants.

Les ICOs se déroulent généralement en trois étapes : l'annonce de l'ICO, l'émission d'un livre blanc présentant la campagne et les conditions de l'offre, puis la vente des tokens. Plusieurs projets ont permis de lever des dizaines de millions de dollars depuis 3 ans, notamment le projet Suisse Tezos (232 millions de dollars).[23] Les tokens auxquels souscrivent les agents lors d'une ICO permettent d'avoir accès à des services de la plateforme émettrice, d'obtenir des droits sur les profits, de voter, de contribuer à la

---

Asset Holding. Ces start-ups mettent en place des solutions reposant sur la blockchain pour gérer des crédits syndiqués, des opérations sur le marché des changes, ou de règlement d'opérations sur titres et dérivés.

[20] Ils ne permettent néanmoins que de garantir l'exécution d'un contrat et ne forment donc pas un contrat au sens juridique du terme (Art 1101, C.Civ).

[21] Ethereum a développé une blockchain disposant d'un langage de programmation turing-complet, ce qui signifie que toutes les fonctions utiles peuvent y être programmées. Le langage offre notamment la possibilité d'écrire des boucles, ce qui n'est pas possible dans le protocole Bitcoin, ce qui oblige à répéter des instructions de façon inefficace.

[22] Il est aussi possible de programmer des smart contracts sur le Bitcoin. Par exemple, la start-up Blockstream a créé un système permettant de programmer des smarts contracts sur le protocole en utilisant des chaînes de blocs parallèles appelées « side chains ».

[23] Adhami, Giudici et Martinazzi (2017) analysent un échantillon de 253 ICOs survenues entre 2014 et Août 2017. Le projet Tezos consiste à développer une blockchain alternative à Bitcoin et Ethereum, reposant sur un système de gouvernance différent.

conception du service proposé. En aucun cas ils ne donnent accès au capital de la société si celle-ci a été créée. Une fois la levée de fonds terminée, les tokens peuvent être revendus sur des marchés secondaires. Un ensemble de services semblables à ceux proposés lors des introductions en bourse s'est développé sur le marché des ICOs. Le devenir de ces activités sera lié à la mise en place d'une réglementation adaptée.[24]

## 3- La blockchain et la création de la confiance

Dans cette partie, nous comparons les mécanismes de création de la confiance dans un système décentralisé, par rapport à un intermédiaire classique.

*La création de la confiance par un intermédiaire*

Un intermédiaire « tiers de confiance » crée par sa présence et son activité les conditions rendant possible l'échange entre deux agents. Par exemple, une banque sert de tiers de confiance pour les transactions de paiement par carte entre acheteurs et vendeurs. Ses activités apportent de la valeur au marché en présence de frictions (comme les asymétries d'information, les coûts d'écriture des contrats, les coûts d'audit, les risques, le coût de l'aléa moral). Son rôle est donc particulièrement important sur les marchés financiers marqués par la présence de coûts de transaction élevés. Le tiers de confiance assume ces tâches grâce à la construction d'une réputation sur le marché. Dans le système financier, la réputation des banques repose d'une part sur le fait qu'elles sont certifiées par des autorités externes comme le régulateur et d'autre part sur la discipline qu'exerce le marché sur leurs comportements.

Une fois que les agents ont choisi d'avoir recours à un tiers de confiance, ce dernier dispose souvent d'un pouvoir de monopole pour réaliser un certain nombre d'activités, comme l'enregistrement des transactions et leur approbation. Avant la transaction, le tiers de confiance collecte et vérifie l'information transmise. Il authentifie les parties prenantes. Pendant la transaction, il enregistre les données et procède éventuellement au règlement. Après la transaction, il permet aux agents de consulter le registre en cas de litige. Par exemple, pour un paiement par carte, les banques authentifient le porteur de la carte en vérifiant l'information transmise. Elles effectuent des transferts de fonds entre l'acheteur et le vendeur. Elles enregistrent la transaction en modifiant les écritures des comptes bancaires des deux parties. Enfin, elles peuvent intervenir en cas de contestation du paiement quand leur responsabilité est engagée.

Le pouvoir centralisé des tiers de confiance sur les données financières comporte des coûts: les frais de transaction pour les consommateurs, les coûts d'entrée sur le marché pour les concurrents, les risques de piratage et de censure. En effet, le tiers de confiance peut exclure d'autres usagers des données dont il dispose, ce qui lui confère un pouvoir de marché. Par exemple, les banques disposent de toutes les données relatives aux paiements effectués par leurs clients. Ces données ont une valeur d'information sur la

[24] Selon H. de Vauplane, il y a des conseillers, des investisseurs et des fonds spécialisés (Polychain), des prestataires de services fournissant des informations (Cryptocurrency Market Capitalization), des agences de ratings (ICO rating), des places de marchés (Kraken), des market makers (Cumberland Minding), des cabinets d'avocats spécialisés (Cooley), des dépositaires de tokens (Ledger). L'AMF a lancé une consultation publique en octobre 2017 sur les ICOs en France.

solvabilité de leurs emprunteurs, ce qui peut créer une barrière à l'entrée sur le marché du crédit pour d'autres entreprises. La centralisation des données expose tout particulièrement le tiers de confiance au risque de piratage (e.g., Target aux Etats-Unis en 2014).[25] Par ailleurs, le tiers de confiance peut refuser d'exécuter certaines transactions, exposant les usagers au risque de censure (Gans et Catalini, 2017).

*La création de la confiance dans un réseau décentralisé*

Dans un réseau décentralisé, les différents participants du réseau se font concurrence pour réaliser les tâches habituellement effectuées par le tiers de confiance : collecter de l'information, vérifier les données, approuver les échanges, enregistrer les transferts de propriété. Il est donc nécessaire de fixer dans le protocole les règles du jeu qui permettront de créer la confiance et d'inciter les membres du réseau à participer à ces différentes activités dans un contexte de concurrence (comme les barrières à l'entrée ou le mode de fixation des prix). Selon le mode de gouvernance de la blockchain, ces règles peuvent être définies soit par un tiers de confiance, soit de façon décentralisée par l'ensemble des membres du réseau, qui approuvent les mises à jour du protocole. Si les acteurs ne parviennent pas à un accord, il peut y avoir une scission du réseau (une fourche) en plusieurs entités.

- *Le choix du degré d'ouverture du réseau*

Il existe deux mécanismes principaux pour créer la confiance dans un réseau décentralisé. Le premier consiste à construire un dispositif d'exclusion autorisant seulement certains membres du réseau à inscrire des informations dans le registre. C'est la solution retenue dans les systèmes de blockchains à permission. Ces blockchains sont souvent utilisées par des groupes d'entreprises décidant de développer des systèmes d'enregistrement partagés.[26] Il existe également des blockchains privées, utilisées par les entreprises qui les ont créées pour des besoins internes. Ces dispositifs ne fonctionnent pas sans une autorité centralisatrice qui décide d'ouvrir ou de fermer l'accès au réseau à certains participants. Leur décentralisation n'est donc que partielle.

Le second mécanisme utilisé dans les blockchains publiques comme le Bitcoin ou Ethereum est plus novateur. Il consiste à laisser le réseau ouvert, en autorisant chaque participant du réseau à valider des transactions. Le protocole doit alors prévoir des mécanismes pour inciter les membres du réseau à entreprendre des activités coûteuses permettant de créer la confiance. Par exemple, les membres peuvent être incités à approuver des transactions par une rémunération qui compense leurs coûts. La plupart du temps, ils sont rémunérés par des unités de comptes internes à la blockchain, des jetons appelés « tokens », dont certains sont des cybermonnaies comme le bitcoin ou l'ether. Le prix de l'activité d'approbation des transactions peut être fixé à l'avance ou varier en fonction de l'offre et de la demande. Pour que la validation des transactions soit crédible, le résultat de cette tâche doit être aussi vérifiable à faible coût. Enfin, pour que le registre soit réputé fiable, sa falsification doit être suffisamment coûteuse pour

[25] En 2014, la chaîne de magasins Target a été piratée, ce qui a entraîné le vol des données de cartes de crédit de 40 Millions d'Américains.

[26] Il existe différents types de blockchains privées, des projets ad hoc comme HyperLedger, des systèmes dérivés des blockchains publiques à usage privé, des blockchains de consortium comme R3, B3i, et des blockchains totalement privées comme BNP Fund Link.

qu'aucun des participants n'ait intérêt à le modifier. Dans les blockchains publiques, la confiance dans l'intermédiaire est donc remplacée par une confiance dans le code du protocole, et les mécanismes d'incitations qui y sont associés.

- *La validation des transactions : coûts et incitations des participants*

Il existe différentes méthodes pour valider les transactions et aboutir à un consensus sur l'état du registre dans une blockchain publique.[27] Le protocole Bitcoin utilise la « preuve de travail ». Cette méthode repose sur une combinaison intelligente de la cryptographie et de mécanismes d'incitation économiques. Son principe consiste à demander aux membres du réseau (« les mineurs ») de résoudre un problème de cryptographie coûteux pour valider des transactions, en contrepartie d'une rémunération.

Le problème de cryptographie peut s'apparenter métaphoriquement à la recherche d'un code secret pour ouvrir une porte sécurisée, soit dans notre cas, ajouter à la chaîne un bloc avec son identifiant[28]. Il existe un mécanisme qui permet d'ouvrir la porte à partir du code secret. Il s'agit d'une fonction de hachage, qui relie le code secret à l'identifiant du bloc. En cryptographie, une fonction de hachage réalise la transformation rapide d'un message (« le code secret ») en une série de caractères (ici l'identifiant du bloc).[29] La validation d'un bloc consiste donc à trouver une séquence de caractères (« le code secret ») dont le hachage par l'algorithme va donner un identifiant débutant par un nombre de zéros prédéterminé.[30] Le code secret est d'autant plus difficile à trouver que le nombre de zéros est élevé, puisqu'il s'agit d'une contrainte plus forte pesant sur le résultat du hachage. Un utilisateur ne peut parvenir à résoudre ce problème qu'en réalisant de très nombreux essais consommateurs de puissance de calcul informatique. En demandant à un utilisateur de fournir une séquence de caractères qui donnera un certain résultat de hachage, le problème est rendu difficile à produire, mais facile à vérifier. En effet, une fois le code secret communiqué à l'ensemble des participants, n'importe quel utilisateur du réseau peut ouvrir la porte rapidement. Pour vérifier la validité du bloc en retrouvant son identifiant, il suffit en effet d'appliquer la fonction de hachage au code secret.

Ce dispositif comporte donc plusieurs avantages. L'usage d'un problème de cryptographie difficile à résoudre permet de réguler la concurrence entre les membres du réseau pour obtenir le droit d'entrer de l'information dans le registre.[31] Il est possible de modifier les paramètres du problème pour influencer les coûts de l'activité

[27] Dans les blockchains privées ou à permission, il n'est pas nécessaire de diffuser les transactions à l'ensemble du réseau pour les valider. Par exemple, la blockchain Corda du consortium R3 fonctionne avec un système de validation direct entre les contreparties.

[28] L'identifiant d'un bloc est appelé "empreinte". Il s'agit d'une étiquette permettant de retrouver n'importe quel bloc entré dans le registre.

[29] Par exemple, avec la fonction de hachage SH-256 de la NSA, le résultat de la fonction est toujours une chaîne de nombres et de caractères (a-f, 0-9) quelque soit la longueur du message reçu.

[30] Cette séquence contient obligatoirement des données relatives au bloc (date, heure, nombre de transactions, identifiant du bloc précédent) ainsi qu'un nombre arbitraire appelé nonce. Le mineur fait varier le nonce inclus dans la séquence jusqu'à ce qu'il obtienne une empreinte satisfaisant la contrainte. Formellement, il s'agit de trouver un nonce N tel que $f(H,T,N)<b$, où b représente l'identifiant du bloc à valider, T un hachage des transactions contenues dans le bloc, H un hachage de l'identifiant du bloc précédent et f la fonction de hachage. Les itérations consistent à faire varier le nonce N contenu dans la séquence, ce qui est très coûteux en énergie et en puissance de calcul.

[31] Cette activité a une structure de tournoi puisqu'il n'y a qu'un seul vainqueur.

de validation des blocs.[32] Enfin, l'asymétrie des fonctions de hachage rend le problème très simple à vérifier, réduisant le coût de vérification de l'information entrée. [33]

Dans le protocole Bitcoin, les mineurs se font concurrence pour gagner le droit d'ajouter un bloc, afin d'obtenir la rémunération prévue en bitcoins.[34] Ce dispositif fonctionne tant que l'espérance de rémunération des mineurs est supérieure aux coûts engagés pour résoudre le problème de cryptographie. La probabilité d'ajout d'une transaction étant croissante avec la puissance de calcul disponible, les mineurs ont intérêt à se regrouper en coalitions pour tenter de maximiser leurs chances d'ajouter le prochain bloc sur la chaîne. Une blockchain fonctionne de façon décentralisée tant qu'aucun groupe de participants n'est suffisamment puissant pour avoir la certitude d'ajouter le prochain bloc.

D'autres protocoles utilisent des procédés différents du Bitcoin pour inciter les membres à participer à la validation des transactions. Dans le mécanisme de « preuve de participation » ou « preuve d'enjeu », les membres sont sélectionnés pour valider les blocs de transaction en fonction de leur degré de participation au réseau, mesuré par exemple par la quantité d'unités de compte détenues.[35] Cette méthode est réputée moins coûteuse en énergie mais plus risquée.

- *L'obtention d'un consensus sur l'état du registre*

L'obtention d'un consensus du réseau sur la validation des transactions se produit au fil du temps avec le mécanisme de la preuve de travail. Il existe en effet toujours une faible probabilité que deux mineurs ajoutent deux blocs simultanément pour valider le même groupe de transactions. Dans ce cas, une fourche (ou bifurcation) apparaît dans la chaîne de blocs, qui se dédouble pendant quelque temps. La règle du protocole consiste à choisir toujours la chaîne la plus longue pour continuer à ajouter les transactions suivantes. Ainsi, il existe toujours une petite chance pour qu'une transaction se trouve dans une branche de la blockchain qui finira par être abandonnée. Dans ce cas, la transaction devra être recommencée. La confiance se construit donc au cours du temps à mesure que la longueur de la blockchain s'accroît. Par exemple, dans le réseau bitcoin, il est conseillé aux usagers d'attendre l'ajout de six blocs environ, soit une heure, afin d'être sûr que la transaction soit enregistrée de façon irréversible. L'obtention d'un consensus du réseau comporte donc un coût lié à une réduction de la vitesse d'exécution des transactions.

- *L'immuabilité du registre : risques de piratage et de fraude*

La règle stipulant que la chaîne la plus longue est toujours conservée dans le réseau augmente le coût de falsification de la blockchain. En effet, si un pirate isolé souhaite

[32] En faisant varier le nombre de zéros exigés, le problème devient plus difficile à résoudre.
[33] Pour consulter le registre des transactions en bitcoin, voir le site blockchain.info.
[34] Actuellement, les mineurs sont rémunérés par 12,5 BTC pour l'ajout d'un bloc. Cette quantité est réduite régulièrement et finira par être remplacée par des frais de transactions lorsque la totalité des bitcoins aura été mise en circulation sur le marché (21 M). Les usagers peuvent déjà choisir d'ajouter des frais de transaction pour faire valider un bloc plus rapidement.
[35] La preuve de participation est utilisée par la cybermonnaie Peercoin combinée avec la preuve de travail. La probabilité de réussite de l'ajout du bloc suivant est proportionnelle à la cybermonnaie que le « forgeur » détient sur son compte.

modifier la chaîne, la seule solution consiste à créer une chaîne de blocs plus longue que la chaîne initiale. Par exemple, supposons que le pirate souhaite falsifier la chaîne à partir du dixième bloc alors que la chaîne en contient seize. Il devra créer six blocs supplémentaires, résolvant ainsi six problèmes de cryptographie coûteux pour parvenir à ses fins. Or, pendant ce temps, le reste du réseau continue à ajouter des blocs à la chaîne la plus longue, et le pirate ne peut parvenir à rattraper le rythme d'ajout des blocs sans alliance avec l'ensemble du réseau. Par conséquent, les mécanismes d'incitation du protocole rendent la fraude a priori impossible à réaliser de façon isolée.

Toutefois, au moins deux types d'attaques sont possibles. La première est une attaque de type « Goldfinger », réalisée par une coalition de participants suffisamment puissante pour prendre le contrôle du réseau et changer la chaîne de blocs. Il faut pour cela que la coalition détienne au moins 51% de la puissance de calcul du réseau. La seconde attaque repose sur la tactique dite du « mineur égoïste ». Elle consiste à ne pas révéler aux autres mineurs la solution à un bloc, tout en continuant à travailler sur une chaîne différente, puis à imposer sa chaîne le moment voulu. Cette attaque est possible avec 25% de la puissance de calcul (voir Eyal et Sirer, 2014). Tant que la part de marché de chaque coalition de mineurs reste suffisamment faible, les coûts de falsification du registre sont trop élevés pour qu'une modification frauduleuse de l'information puisse être effectuée. Néanmoins, en l'absence d'une autorité externe capable de surveiller la concentration du marché, il existe un risque qu'un groupe de participants prenne le pouvoir sur le réseau.

## 4- La blockchain et les coûts de l'intermédiation financière

La blockchain pourrait réduire les coûts des activités opérées par les intermédiaires financiers. Selon Gans et Catalini (2017), la blockchain permet une réduction des coûts d'audit des transactions et des coûts de mise en réseau des participants à un système financier. La blockchain pourrait également réduire les coûts associés à la sécurisation des échanges financiers, améliorer la vitesse de traitement de certaines transactions et permettre une flexibilité sur les opérations de règlement et de compensation réalisées par les infrastructures post-marché.

*Les coûts de mise en réseau des participants à un système financier*

En offrant aux usagers la possibilité de payer dans un réseau de pair à pair, la blockchain va réduire les coûts de mise en réseau des utilisateurs des systèmes de paiement de détail. De nombreuses fintechs proposent des solutions innovantes reposant sur la blockchain pour les paiements entre clients particuliers: les portefeuilles offrant des services de paiement de pair à pair (Mycelium, BitPay…), les plateformes d'échanges de bitcoins et d'autres cybermonnaies (Coinbase), les services de transferts de fonds internationaux (BitPesa, Abra, Rebit). Les institutions financières commencent également à utiliser la blockchain pour développer des systèmes de paiement de pair-à-pair et de transferts de devises entre particuliers plus efficaces.

La valeur associée à la mise en réseau de participants à un système financier ne se limite pas au domaine des paiements. En effet, la blockchain permet plus largement de développer des places de marché fonctionnant sans intermédiaires avec leurs propres systèmes d'incitations et de rémunérations, réduisant le coût de mise en réseau des

participants à un projet (Gans et Calalini, 2017). Par exemple, le Hedge Fund Numerai attire les contributions de data scientists pour améliorer ses modèles de prédiction en les rémunérant avec un smart contract en fonction de la performance de leurs propositions.

*L'amélioration de la vitesse de traitement des transactions en question*

Pour l'instant, les blockchains publiques n'ont pas résolu le problème du traitement rapide des transactions à grande échelle.[36] Par exemple, le temps de traitement des transactions en bitcoins est actuellement plus long que pour les systèmes de paiement par carte gérés par Visa et MasterCard.[37] Des évolutions du protocole pourraient modifier cette tendance, avec l'usage de sidechains comme le propose la société Blockstream ou de changements de méthode pour aboutir à un consensus. Toutefois, un nouveau standard pour réaliser des transactions à grande échelle ne peut s'imposer sans un consensus de la majorité des nœuds du réseau. Une guerre des standards a opposé au sein du protocole Bitcoin les partisans d'une augmentation de la taille des blocs (e.g., Bitcoin Unlimited) et les partisans d'une réduction des données enregistrées par transaction (e.g., Segwit), freinant l'adoption d'une solution permettant de réduire les temps de traitement sur le réseau.[38] Cet exemple illustre les limites de l'efficacité des blockchains publiques et de l'open source. Faute d'un consensus entre l'ensemble des participants, les fourches du protocole réduisent la valeur associée à la mise en réseau et freinent l'innovation.

En revanche, le temps de traitement des transactions financières impliquant plusieurs participants pourrait être réduit sur les blockchains privées, fonctionnant sans mécanisme de consensus (pour les transferts de devises et les prêts syndiqués).[39] Par exemple, le temps pour réaliser une opération de prêts syndiqués pourrait passer d'une vingtaine de jours à moins d'une semaine grâce à l'usage d'une blockchain. De même, le temps de traitement pour les transferts de devises pourrait être réduit. Selon Philippe Denis (BNP Paribas), « La blockchain évite les correspondances entre les banques, les délais incertains et les risques d'erreurs. Le temps de transfert s'établit à 90 minutes contre 1 à 6 jours pour un transfert (de devises) traditionnel ».[40] BNP Paribas s'appuie aussi sur la technologie blockchain pour proposer un traitement des lettres de crédit plus rapide (Smart LC), ou pour gérer de façon plus efficace le « collatéral » dans des opérations de commerce international des matières premières (Collat'Shaker).

*La réduction du coût de la liquidité et la création de nouveaux marchés*

Pour les activités de post-marché, la technologie blockchain permet une flexibilité dans le choix des temps de règlement et de compensation, améliorant ainsi la liquidité, tout en réduisant les besoins en collatéral pour l'échange des titres les plus risqués. Pour certains titres, les opérations de compensation et de règlement pourraient être

[36] On parle du problème de la « scalabilité ».
[37] Le Bitcoin permet de gérer sept transactions par seconde, PayPal 100 et Visa entre 2000 et 7000.
[38] Pour comprendre le lien entre la taille des blocs et le mécanisme d'incitation des mineurs, voir Houy (2014).
[39] Source: rapport de l'ESMA « blockchain and securities markets ».
[40] BNP Paribas a développé un système pour gérer les transferts de devises sur une blockchain "Cash Without Borders".
Source : https://atelier.bnpparibas/fintech/article/blockchain-heure-premieres-realisations

effectuées quasiment instantanément, ce qui réduira les coûts de traitement post-marché.[41]
En améliorant la traçabilité des échanges de titres financiers, la blockchain permettra de créer des bourses d'échanges de titres pour des segments de clientèle qui n'étaient pas couverts jusqu'à présent par l'offre des intermédiaires. Par exemple, BNP Paribas Securities Services et la plateforme de crowdfunding SmartAngels ont développé une blockchain permettant de créer un marché secondaire sur les échanges de titres des sociétés non cotées. Le rapport de Paris Europlace (2017) affirme même qu'à terme, une blockchain pourrait tenir le rôle de bourse, de chambre de compensation, de dépositaire central, et de système de règlement-livraison. Toutefois, de nombreuses questions pratiques restent à résoudre avant que l'infrastructure actuelle des places boursières ne soit remplacée.

*La sécurisation des transactions et la gestion des pseudonymes*

La sécurisation des échanges par la cryptographie pourrait aussi créer de la valeur. Notamment, Fung et Halaburda (2016) identifient différents types de paiements électroniques abandonnés actuellement par les consommateurs pour préserver leur vie privée ou réduire les risques de piratage. La technologie blockchain est-elle plus efficace pour préserver la vie privée et réaliser des échanges sécurisés ? Cette affirmation commune doit être nuancée. Le choix de la méthode pour aboutir à un consensus influence le niveau de sécurité. Par exemple, le mécanisme de preuve de détention est réputé plus rapide et moins sûr que la preuve de travail. Il existe en effet un arbitrage dans le mécanisme de certification des transactions entre la sécurité et la rapidité du système. Par ailleurs, le respect absolu de l'anonymat n'est pas toujours garanti, car il est possible de croiser des données pour retrouver les utilisateurs récurrents de cybermonnaies par leurs adresses (Reid et al., 2012). Enfin, les consommateurs sont responsables de leur propre protection contre le vol et le piratage, ce qui nécessite de traiter avec vigilance leurs clés privées.[42]

*Les coûts d'audit et de conformité avec la réglementation financière*

Avec la blockchain, les banques et les institutions financières pourront réduire les coûts d'audit et de réconciliation associés aux échanges impliquant de nombreux intermédiaires. Les transactions seront en effet enregistrées dans un registre unique, traçable et vérifiable à faible coût. L'information y est disponible de façon non rivale. Les coûts d'audit pourraient devenir quasiment nuls pour les échanges d'actifs digitaux. La mise en œuvre de smart contracts pourrait aussi réduire les risques de contentieux. Toutefois, les tiers de confiance et les auditeurs continueront à jouer un rôle pour réconcilier les entrées dans le registre avec le monde réel, quand les enregistrements concernent des actifs physiques.

[41] La société SETL a développé une solution permettant la compensation instantanée des positions de change. Le choix du rythme de compensation pourrait être paramétré dans une blockchain : « I can even think we (…) allow participants to select the pace at which they want to settle » -Fredrik Voss, VP of blockchain innovation at Nasdaq.
[42] Pour une analyse de la responsabilité des acteurs du système financier en cas de piratage de la blockchain, voir le rapport de Paris Europlace (2017).

La blockchain pourrait également faire diminuer les coûts associés au respect des réglementations financières. Par exemple, les coûts du reporting réglementaire sur les marchés financiers pourront être réduits en octroyant au régulateur des droits spéciaux d'accès au registre pour certaines opérations (en respect des réglementations EMIR et MIF). Les coûts de vérification de la conformité pourront aussi diminuer. Ainsi, le partage de documents comme les cartes d'identité ou les dossiers fiscaux entre plusieurs banques dans un registre sécurisé distribué pourrait permettre de mieux répondre aux exigences réglementaires concernant les procédures de connaissance de leurs clients (KYC Know Your Customer) et de lutte contre le blanchiment d'argent et le financement du terrorisme (AML Anti Money Laundering). Certaines regtechs proposent des services innovants aux banques reposant sur la blockchain pour réduire les coûts associés à la conformité et au reporting. Elles travaillent parfois étroitement avec le régulateur financier pour proposer des solutions de régulation automatisées sur la blockchain. Au Royaume-Uni, la Financial Conduct Authority (FCA) a notamment développé des solutions de reporting réglementaire avec des entreprises regtechs dans le cadre du programme BARAC (Blockchain Technology for Algorithmic Regulation and Compliance).[43]

## 4- Les problématiques réglementaires

La réglementation de la blockchain comporte plusieurs enjeux, dont nous esquissons les contours dans cette partie.[44] D'une part, les régulateurs doivent limiter les risques associés au déploiement des blockchains publiques (e.g., Bitcoin, Ethereum) et des nouveaux services qui leurs sont associés. D'autre part, ils doivent construire un cadre permettant une reconnaissance légale des opérations réalisées sur les blockchains privées, afin que les intermédiaires financiers puissent bénéficier de la baisse des coûts apportée par la technologie. Chaque autorité de régulation doit choisir des mesures permettant de créer un équilibre entre la protection des consommateurs, l'ouverture à la concurrence du secteur financier aux start-ups de la fintech et les incitations à l'innovation.[45]

*La réglementation des risques associés aux cybermonnaies*

Les cybermonnaies comme le bitcoin comportent différents risques pour les consommateurs et pour les institutions financières. Dans de nombreux pays et juridictions (e.g., France, Europe), elles ne peuvent pas être qualifiées de monnaies au sens juridique, ni même au sens économique (Yermack, 2015).[46] Par conséquent, les

[43] Source: https://www.fca.org.uk/firms/regtech/our-work-programme. La FCA a développé dans le 'Project Maison' en partenariat avec le consortium R3 et plusieurs banques une solution regtech reposant sur la blockchain pour suivre le marché du crédit immobilier. Un autre projet (SmartReg) étudie l'usage de smart contracts pour vérifier la conformité.

[44] Pour un état des lieux plus complet des règles en vigueur et de la position des régulateurs, voir le rapport de Paris Europlace (2017).

[45] Les approches des régulateurs concernant la réglementation des fintechs diffèrent d'un pays à l'autre. Certaines autorités (FCA par exemple) ont mis en place une « sandbox ». Il s'agit d'un système de sélection des projets innovants donnant lieu à une coopération entre le régulateur et les entreprises choisies. Les entreprises sont exemptées de contraintes pendant la durée de l'expérimentation.

[46] Elles ne peuvent ni être qualifiées de monnaie au sens de l'article L.111-1 du Code Monétaire et Financier, ni de monnaie électronique au sens de la directive du 16 septembre 2009, ni de monnaie locale complémentaire au sens de la loi n°2014-856 relative à l'économie sociale et solidaire.

consommateurs ne peuvent pas être certains qu'ils pourront les utiliser pour payer chez des marchands ou les convertir en monnaie légale. Le bitcoin n'est pas assorti d'une garantie légale de remboursement à tout moment et à sa valeur nominale. En outre, le cours des cybermonnaies est très volatile, ce qui nécessite d'avertir les consommateurs des risques de perte associés à leur détention. Les plateformes d'échange de bicoins ne proposent aucune garantie de liquidité ni de cours légal. Elles risquent aussi de faire faillite si elles ne sont pas suffisamment vigilantes aux risques de piratage.[47] Par ailleurs, aucune autorité ne veille à la mise en place des conditions nécessaires à la sécurité du stockage des clés permettant l'échange de bitcoins.[48]
Les cybermonnaies permettant de réaliser des transactions sous des pseudonymes, elles risquent de favoriser les activités illégales et le blanchiment d'argent, comme en témoigne la fermeture en 2013 par le FBI du site Silk Road aux Etats-Unis, qui permettait à des usagers de financer des activités frauduleuses en bitcoins. En France, les plateformes convertissant des bitcoins en monnaie ayant cours légal doivent être agréées par l'ACPR comme prestataires de services de paiement (29 septembre 2014). Les plateformes doivent donc respecter les règles de lutte contre le blanchiment et le financement du terrorisme (LBC-FT) et sont surveillées par la Banque de France. Aux USA, le département du Trésor FinCEN demande aux plateformes de détenir une licence de Money Service Business.

*La réglementation des ICOs*

Plusieurs régulateurs envisagent de réguler ou d'interdire les ICOs.[49] Il existe en effet de nombreux risques associés à ces opérations de levées de fonds en cybermonnaies. Les sociétés levant des fonds par ICOs pourraient fournir une documentation inexacte, réaliser du blanchiment d'argent. Par ailleurs, les investisseurs pourraient choisir d'acheter des tokens sans être conscients des risques de perte en capital, de volatilité des cours ou de fraude. En outre, il n'existe pas encore de définition juridique pour les tokens.[50] Aux Etats-Unis et à Singapour, les régulateurs ont jugé qu'ils pourraient être considérés au cas par cas comme des titres financiers.

*La problématique de la réglementation des blockchains publiques*

La création de règles contraignantes pour l'usage des blockchains publiques comme celle du Bitcoin est complexe à mettre en oeuvre. En effet, pour réguler une blockchain, il faudrait pouvoir contrôler la localisation des serveurs, l'activité des mineurs, l'intégrité des algorithmes ou identifier les parties effectuant des transactions.[51] Or, les utilisateurs des blockchains publiques opèrent sous des pseudonymes et sont dispersés entre différents pays. Il est donc difficile d'établir leur responsabilité en cas d'incident ou de fraude. Les blockchains publiques soulèvent aussi de nombreuses questions

[47] En février 2014, la plateforme Mt.gox a déposé le bilan après s'être fait dérobé plus de 850 000 bitcoins valorisés à l'époque à 350 millions d'euros.
[48] Il existe des solutions de marché permettant de stocker les clés permettant d'échanger des bitcoins de façon sécurisée, comme celle proposée par la société Ledger.
[49] La Chine a interdit les ICOs, la Financial Conduct Authority (RU) les autorise au cas par cas, l'Autorité des Marchés Financiers en France a lancé une consultation publique en octobre 2017.
[50] Devant cette incertitude juridique, les principaux acteurs mondiaux des cryptomonnaies se sont associés pour tenter de s'autoréguler en créant le « blockchain token securities law framework ».
[51] Voir Bonneau et Renard (2017) pour une analyse juridique.

juridiques relatives au traitement des données personnelles. Par exemple, il est difficile d'appliquer le droit à la rectification, à la suppression ou à l'oubli des données.[52]
Par ailleurs, le principe même d'une blockchain publique est de laisser le code ouvert à toute modification, sans aucun contrôle de l'intégrité ni de la qualité des changements apportés. L'affaire du détournement de 50 millions de dollars du fonds d'investissement décentralisé « The DAO » qui avait levé des fonds en ether est emblématique des difficultés posées par l'ouverture du code informatique. Le pirate a en effet profité d'une défaillance du code, menaçant de procès tous ceux qui tenteraient de récupérer la monnaie dérobée en vertu de la logique «The Code is law » (Lessig, 2006). Dans l'univers des cybermonnaies, est-il souhaitable et possible que le code informatique se substitue aux tiers de confiance ? En effet, le code présente toujours des points de vulnérabilité, parce qu'il est entré par la main de l'homme.

*La reconnaissance des opérations réalisées sur les blockchains à permission ou privées*

L'usage des blockchains privées ou de blockchains à permission comporte moins de risques que celui des blockchains publiques, car chaque membre du réseau peut être clairement identifié et désigné comme responsable de ses actions. Toutefois, le régulateur doit aussi créer un cadre légal pour reconnaître les opérations réalisées sur une blockchain. Depuis Avril 2016, la blockchain est reconnue en France pour enregistrer et céder des opérations sur les minibons (article L223-12 du Code Monétaire et financier).[53] La Direction Générale Trésor a aussi proposé en octobre 2017 un projet d'ordonnance permettant de faciliter la transmission de certains titres financiers par la blockchain.[54] L'ordonnance a été adoptée le 8 décembre 2017.

## Conclusion

La blockchain va conduire à une évolution du rôle des tiers de confiance dans la finance mais ne conduira pas à leur disparition. Cette innovation apportera de nombreux bénéfices au système financier en réduisant la concentration du pouvoir des intermédiaires sur l'information, en apportant plus de transparence pour l'audit et le contrôle des états financiers, en favorisant l'émergence de services et de modes de financement novateurs. Pour que la société puisse bénéficier de cette innovation, le régulateur devra fixer un cadre limitant les risques qui y sont associés, voire innover lui-même dans ses pratiques de contrôle des informations financières.

[52] Voir le document de l'Open Data Institute ODI-TR-2016-001.
[53] Ord. n° 2016-520, 28 avr. 2016, relative aux bons de caisse, JO 29 avr.
[54] Un alinéa est ajouté à l'article L. 228-1 *: «* Lorsque les statuts de la société l'y autorisent, ces valeurs mobilières peuvent être inscrites dans un dispositif d'enregistrement électronique partagé, conformément à l'article L. 211-3-1 du Code monétaire et financier »

**Bibliographie**


Adhami, S., Giudici, G., Martinazzi, S. (2017) : 'Why do businesses go crypto ? An empirical analysis of Initial Coin Offerings'.

Autorité des Marchés Financiers (octobre 2017) : Document de consultation sur les Initial Coin Offerings (ICOs).

Babbitt, D., Dietz, J. (2015) : « cryptoeconomic design : A proposed agent-based modeling effort », working paper.

Böhme, R., Christin, N., Edelman, B. (2015) : « Bitcoin : economics, technology, governance, » Journal of Economic Perspectives, 29(2) : 213-38.

Bonneau, T., Renard, I. (2017) : « Fonctionnement de la Blockchain – Compatibilité avec un environnement réglementé : que peut-on et que doit-on réglementer dans une Blockchain ? », Revue de Droit bancaire et financier n° 1, Janvier 2017, dossier 3.

Bresnahan, T, Trajtenberg M (1995) 'General purpose technologies « Engines of growth » ?', Journal of Econometrics, vol.65, n.1, pp. 83-108.

Buterin, V. (2015) 'Visions part I : The value of blockchain technology', White Paper.

Collomb, A., Sok, C. (2016) : « Blockchain et autres registres distribués : quel avenir pour les marchés financiers ? », Opinions et débats, publication de l'Institut Louis Bachelier.

Davidson, Sinclair and De Filippi, Primavera and Potts, Jason, 'Economics of Blockchain' (March 8, 2016). Available at SSRN: https://ssrn.com/abstract=2744751 or http://dx.doi.org/10.2139/ssrn.2744751

Eyal I., Sirer E.G. (2014): "Majority Is Not Enough: Bitcoin Mining Is Vulnerable". In: Christin N., Safavi-Naini R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science, vol 8437. Springer, Berlin, Heidelberg.

European Securities and Markets Authority (2017): "The Distributed Ledger Technology applied to Securities Markets". Available at: https://www.esma.europa.eu

Freixas, X., Rochet, J.C. (2008): "Microeconomics of Banking", the MIT Press.

Fung, Ben S.C., Halaburda, Hanna (2016) : « Central Bank Digital Currencies: A Framework for Assessing Why and How", Bank of Canada Staff Discussion Paper.

Gandal, N. and Halaburda, H. (2014): "Competition in the Cryptocurrency Market". CEPR Discussion Paper No. DP10157. Available at SSRN: https://ssrn.com/abstract=2501640

Gans, J., Catalini, C. (2017): "Some Simple Economics of the Blockchain." Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16. Available at SSRN: https://ssrn.com/abstract=2874598

Halaburda, Hanna, Sarvary, Miklos (2015): "Beyond bitcoin: the Economics of Digital Currencies", Palgrave Macmillan.

Harvey, Campbell R. (2016): "Cryptofinance", Working Paper.

Houy, Nicolas, (2014): "The economics of Bitcoin transaction fees", Gate Working paper n.1407.

Lessig, L. (2006): Code version 2.0, New York : Basic Books.

Nakamoto, S. (2008) 'Bitcoin : A peer-to-peer electronic cash system', Working Paper, disponible sur : https://bitcoin.org/bitcoin.pdf

Open Data Institute (2016): 'Applying blockchain technology in global Data infrastructure' ODI-TR-2016-001.

Paris Europlace : « Les impacts des réseaux distribués et de la technologie blockchain sur les activités de marché », Rapport datant d'octobre 2017.

Philippon, T., 2016. The FinTech Opportunity. NBER Working Paper n°22476.

Pilkington, M. (2016) : « Blockchain technology : Principles and Applications » in F.X. Olleros and M. Zhegu (eds) Research Handbook on Digital Transformations, Edward Elgar.

Reid, F. et Harrigan M. (2013) : « An Analysis of Anonymity in the Bitcoin System, » in Y. Altchuler, Y. Elovici, A.B. Cremers et al. (eds), Security and Privacy in Social Networks, Springer, p.197-223.

Schuh, Scott, Shy, Oz (2016): "U.S. Consumers' Adoption and Use of Bitcoin and other Virtual Currencies," Working Paper.

Vauplane, H. (2017): "Crypto-assets, Token, Blockchain, ICO: un nouveau monde?", Blockchain daily news, disponible sur: https://www.blockchaindailynews.com/Crypto-assets-Token-Blockchain-ICO-un-nouveau-monde_a25783.html

Waelbroeck, P. (2017): "Les enjeux économiques de la blockchain", Annales des Mines – Réalités Industrielles, 2017/3, p.10-19.

Wright, A., De Filippi, P. (2015): "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", Working Paper.

Yermack, D. (2015): "Is Bitcoin a Real Currency?" in David K.C. Lee ed., The Handbook of Digital Currency (Elsevier, 2015), p.31-44.