RÉALITÉS INDUSTRIELLES

« Se défier du ton d'assurance qu'il est si facile de prendre et si dangereux d'écouter »
Charles Coquebert, Journal des mines n°1, Vendémiaire An III (septembre 1794)

Blockchains et *smart contracts* : des technologies de la confiance ?

UNE SÉRIE DES
ANNALES DES MINES
FONDÉES EN 1794

AOÛT 2017

Publiées avec le soutien de l'Institut Mines-Télécom

UNE SÉRIE DES

ANNALES DES MINES

FONDÉES EN 1794

RÉALITÉS INDUSTRIELLES

Série trimestrielle • Août 2017

Photo de couverture :
Circulation des données, illustration.
Photo © First signal/ISTOCK-GETTY IMAGES

Iconographie
Christine de Coninck

Abonnements et ventes
COM & COM
Bâtiment Copernic - 20 Avenue Edouard Herriot
92350 LE PLESSIS ROBINSON
Alain Bruel
Tél. : 01 40 94 22 22 - Fax : 01 40 94 22 32
a.bruel@cometcom.fr
Mise en page : Nadine Namer
Impression : Printcorp

Editeur Délégué :
FFE – 15 rue des Sablons - 75116 PARIS - www.ffe.fr

Régie publicitaire : Belvédère Com
Fabrication : Charlotte Crestani
charlotte.crestani@belvederecom.fr - Tél. : 01 53 36 20 46
Directeur de la publicité : Bruno Slama
Tél. : 01 40 09 66 17
bruno.slama@belvederecom.fr

SOMMAIRE

Blockchains et *smart contracts* : des technologies de la confiance ?

Blockchains et *smart contracts* : des technologies de la confiance ?

SOMMAIRE

Les *smart contracts* et les *oracles*

Les opportunités, les enjeux

Le dossier est coordonné par Jean-Pierre DARDAYROL

Avant-propos

Par Jean-Pierre DARDAYROL
Ingénieur général des mines, président du comité de rédaction d'*Enjeux numériques* (nouvelle série des *Annales des Mines*)

La préparation de chaque numéro des *Annales des Mines* est pour son coordonnateur et la Rédaction une (petite) aventure, un cheminement qui tout en donnant corps au thème choisi un an auparavant apprend et montre beaucoup.

Partager les enseignements, les étonnements de notre travail est certainement une introduction qui prépare à la lecture structurée des articles de ce numéro consacré à la *blockchain*, ou chaîne de blocs, et à ses cas d'usage.

Le voyage exploratoire que nous vous proposons est double : le premier parmi les acteurs du numérique, le second dans l'univers en construction de la *blockchain*.

En ce qui concerne les acteurs, un constat s'impose avec force : les acteurs – entreprises, administrations, monde académique, etc. – sont mobilisés par le sujet dans une posture, le plus souvent, pro-active et dynamique.

Cette mobilisation nous est apparue plus précoce, plus large que celle constatée les années précédentes sur les innovations numériques venues sur le devant de la scène, comme l'infonuagique. Peut-être est-ce le signe de l'appropriation et de la maîtrise croissante du numérique par notre société ?

Deuxième constat, les réflexions et réalisations en cours sont portées par des acteurs de tous types, deux groupes étant particulièrement actifs : les grands acteurs historiques et les *start-ups* ; on notera à ce propos que les entreprises et les institutions fondées avant 1900, d'une part, et les *start-ups*, d'autre part, ont donné chacune plus du tiers des articles de ce numéro. Les Universités et les Écoles se sont d'ailleurs impliquées avec une grande diversité de sujets, de personnes (enseignants-chercheurs et étudiants) et de types d'institution.

Cependant, l'observation attentive des projets et des réalisations montre une forme de différenciation générationnelle au demeurant perçue par certains des auteurs : les personnes et les organisations les plus jeunes adoptent vis-à-vis de la *blockchain* et plus encore des *smart contracts* une politique que l'on pourrait qualifier d'appropriation directe et « décomplexée », alors que les organisations porteuses d'actifs et de processus historicisés adoptent, en général, des démarches plus exploratoires – qui s'inscrivent néanmoins dans des politiques audacieuses et innovantes.

On voit donc se dessiner dès à présent à l'occasion de l'arrivée de la *blockchain*, au-delà de l'aspect générationnel, le désir d'un renouvellement de l'innovation, de la compétition et de la concurrence des services et des acteurs dans de nombreux secteurs.

Le second cheminement nous conduit « dans » la *blockchain*. Il apparaît immédiatement que le mot *blockchain* ne désigne ni une innovation ni un objet, mais la combinaison intelligente, inédite, variable selon les acteurs, des services et des plateformes de technologies existantes pour créer une « gestion collaborative d'un registre distribué », un système permettant de créer une certaine confiance entre acteurs sans recourir à une gouvernance et à une organisation centralisée investie de pouvoirs larges et exorbitants.

Dans le monde de la confiance, dans celui des bases de données, tous deux marqués par plusieurs décennies de stabilité des modèles et des modes de pensée, la novation est radicale. Elle s'inscrit hors des savoir-faire, des cadres juridiques, des modèles d'affaires, des infrastructures installées largement disponibles.

Les articles montrent qu'elle permet de s'interroger sur de nombreuses relations ou processus de natures variées – *Business to Business* (B2B), mais plus encore *Business to Consumer* (B2C), *Administration to Consumer* (A2C), *Consumer to Consumer* (C2C), à des fins de confiance évidemment mais aussi d'efficience et d'efficacité, de fiabilisation des données, de traçabilité, de contrôle interne ou externe, qu'il s'agisse de processus existants ou d'innovations.

Aujourd'hui, au vu des travaux et des services expérimentaux en construction ou en test, il est bien téméraire d'anticiper qui seront les élus et qui ne le seront pas.

Les *smart contracts* méritent une attention toute particulière. Greffés sur les infrastructures des chaînes de blocs, ce ne sont pas des contrats mais des logiciels d'assistance à la préparation, à l'exécution et à la supervision de contrats. Leur promesse est d'aider à la massification des relations contractuelles. Cependant, les analyses des auteurs indiquent qu'ils doivent encore être mieux compris et expérimentés avant d'être éventuellement mis en opération.

Il en est de même des « oracles », sources d'informations externes aux *blockchains*, dont la sécurisation et l'interfaçage avec le monde physique sont cruciaux.

Ce numéro tourné vers des avenirs nouveaux est particulièrement riche. C'est heureux : il est le dernier numéro de *Réalités industrielles* à être consacré exclusivement au numérique. L'intention des *Annales des Mines* n'est nullement de déserter le champ du numérique, mais bien au contraire de l'investir plus intensément en lançant en mars 2018 une nouvelle série trimestrielle, la quatrième, consacrée entièrement au numérique : *Enjeux numériques*/*Digital issues*. L'intelligence artificielle, l'IA, sera le sujet du premier numéro ; l'économie et la régulation des données sera le thème du deuxième. *Enjeux numériques*/*Digital issues* sera publié sur papier en français avec une nouvelle maquette et, presque simultanément, en français et en anglais sur le *Web*. N'hésitez pas à vous exprimer sur ce projet auprès de la Rédaction.

Bonne lecture de ce numéro, de cette chaîne d'articles.

La *blockchain* : concept, technologies, acteurs et usages

Par Côme BERBAIN
Sous-directeur adjoint Expertise à l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

La *blockchain* est à la mode : difficile, en effet, d'ignorer ce terme utilisé en abondance, dans des acceptions variées ! Afin d'appréhender ce nouveau phénomène, il est nécessaire de tenter de le définir, d'identifier ses éléments structurants et de s'interroger sur la pertinence de ses propriétés et de ses promesses.
La multitude des expérimentations dans un grand nombre de secteurs économiques nous invite à nous interroger sur la pertinence de l'utilisation de la *blockchain* en fonction des cas d'usage, et sur les motivations réelles des différents acteurs.
Bien loin d'être uniquement techniques, les enjeux fondamentaux de la *blockchain* ont trait à l'organisation, à la gouvernance et à la définition même des solutions permettant de répondre à la question de la confiance dans les interactions humaines. En ce sens, la *blockchain* est un nouvel outil technique qui induit et participe à la transformation numérique de nombreux secteurs, en particulier de celui des métiers du droit.

Un seul concept recouvrant plusieurs technologies

La confiance entre des acteurs réalisant des transactions repose généralement sur un système centralisé : les acteurs, ne pouvant se faire confiance mutuellement, choisissent de faire confiance à une entité qu'ils reconnaissent tous (État, banque, notaire…). Ce tiers de confiance tient un registre de leurs transactions, garantissant ainsi la régularité de leurs échanges. En fonction du type de transactions, l'accès au registre peut être libre pour tous, ou restreint à certains acteurs. Dans tous les cas, le tiers de confiance détient le monopole de la mise à jour du registre des transactions afin d'écarter tout risque de fraude.

Le concept de la *blockchain* est de proposer des extensions de ce modèle centralisé permettant une gestion collaborative d'un registre distribué et de s'abstraire ainsi de la nécessité d'une autorité centrale de confiance. Ce concept repose sur deux caractéristiques :

- le registre est implanté à l'aide d'une « chaîne » de blocs de données décrivant les transactions, liés entre eux par un procédé cryptographique (d'accès public, ce registre est généralement décentralisé) ;
- tout utilisateur peut ajouter des éléments au registre. Ces éléments sont assemblés sous la forme de blocs, et il existe un processus permettant de valider de manière définitive les nouveaux blocs au fur et à mesure que ceux-ci sont ajoutés à la « chaîne » : ce processus vise à empêcher la falsification du registre et est en général également public et réalisé de manière décentralisée.

Plusieurs technologies (Bitcoin, Ethereum, Ripple…) se sont construites autour de ce paradigme. Elles s'appuient sur des briques techniques préexistantes (registre distribué, signature électronique, cryptographie asymétrique, preuve de travail, machines virtuelles…), l'innovation résidant dans leur assemblage.

Plus précisément, les éléments structurant les différentes technologies de *blockchain* existantes sont au nombre de quatre :

- le registre et son contenu : le registre étant une forme de stockage distribué, il est possible d'y inclure des éléments de diverses natures. L'utilisation du registre pour répertorier des transactions demeure le cas majoritaire. Néanmoins, il est possible d'y stocker aussi bien des fichiers que des communications. Les *smart contracts* [(1)] permettent d'étendre la notion de stockage distribué à celle de capacité de calcul distribué ;
- l'accès au registre pour les différents acteurs : la publicité (chaîne publique, chaîne privée ou chaîne en consortium), le type des acteurs (personnes morales ou personnes physiques) et l'identité affichée (réelle ou pseudonymique) des acteurs en sont les principaux paramètres. Deux types d'acteur se distinguent : les utilisateurs et les valideurs ;

(1) Un smart contract *est un contrat formalisé sous la forme de codes informatiques stockés dans une technologie de* blockchain *et dont l'exécution est automatique, dès lors que les conditions en sont réunies.*

- la validation du registre par consensus (le terme de « consensus » doit être pris ici dans son acception anglo-saxonne) : en fonction des mécanismes de validation choisis, la possibilité pour l'ensemble des acteurs de contribuer à l'émergence du consensus (ou celle d'exprimer un désaccord) ne peut être garantie. L'ensemble des acteurs partage cependant un accord sur l'état du registre. Plusieurs méthodes de validation distribuée aux propriétés distinctes coexistent : preuves de travail, preuve de participation (*proof of stake*), consensus fédéré… ;
- la régulation des acteurs : afin d'inciter les acteurs à contribuer à la communauté (notamment en mettant à disposition des moyens informatiques), mais également afin d'obtenir un équilibre du système, il est nécessaire de mettre en place un mécanisme de régulation ; le plus souvent, celui-ci repose sur une monnaie (associée à la technologie retenue).

Chaque technologie correspond à des choix en matière de solutions retenues pour ces différentes problématiques. L'effectivité des promesses de la *blockchain* dépendant de ces choix, elle ne peut être évaluée que pour une technologie donnée. Le Tableau ci-dessous illustre ces choix, pour trois technologies.

	Bitcoin	Ethereum	Ripple
Contenu	Transactions monétaires	Transactions, *Smart Contracts*	Transactions financières
Accès	Public	Public	Restreint au monde financier. Publicité des informations de transaction, mais pas des informations de paiement
	Pseudonyme	Pseudonyme	Identité réelle
Validation	Preuve de travail	Preuve de travail – en transition vers un modèle de preuve de participation	Vote sur la correction des transactions entre les valideurs (avec un seuil de 80 %)
Régulation	Génération de nouveaux bitcoins et ajustement de la difficulté de la preuve de travail	Rémunération en éther. Consommation de gaz en fonction de la quantité de calcul distribué dans les *smart contracts*	Monnaie associée XRP (*Ripples*)

Les propriétés et leurs limites structurelles

La principale promesse de la *blockchain* est la décentralisation de la confiance, qui permet la disparition du tiers de confiance teneur du registre. Cette promesse repose sur l'infalsifiabilité du registre : tout élément inséré dans le registre est immuable, il ne peut être ni supprimé ni même modifié. Le système préserve également l'ordre de validation des différents éléments. Cette infalsifiabilité structurelle porte en elle sa propre limite en matière de gestion des contentieux : même des transactions qui correspondraient à des actions illégales ou contestées ne peuvent être supprimées, seule une correction de leurs effets peut être apportée au moyen de nouvelles transactions.

Le processus de validation, qui vise à garantir l'infalsifiabilité, est donc la pierre angulaire des différentes technologies. Fonctionnellement, il correspond à l'émergence d'un consensus entre l'ensemble des valideurs, et ce, sur chaque nouveau bloc (malgré la présence potentielle d'acteurs non coopératifs ou malveillants) : cela renvoie à un problème mathématique connu, celui dit des généraux byzantins, qui doivent correspondre entre eux par messages conçus sur la base d'un algorithme et gagner ainsi la bataille même s'il y a parmi eux des traîtres. Néanmoins, il n'existe pas de lien démontrable entre ce problème théorique et les solutions utilisées par les différentes technologies existantes.

Le caractère distribué du registre induit une transparence et une auditabilité des éléments pour les acteurs. Dans le cas de technologies publiques, cela confère un avantage majeur quant à la confiance des acteurs, mais peut limiter les types de données manipulables, telles que des données à caractère personnel [(2)]. À l'inverse, dans le cas de technologies ou de déploiements privés, seuls les acteurs impliqués bénéficient de cette propriété.

L'infalsifiabilité et la transparence engendrent une caractéristique supplémentaire de résilience des systèmes utilisant ces technologies : en cas d'incident ou d'atteinte majeure, tout acteur est en mesure de créer un nouveau système à partir d'un état sur lequel le consensus est assuré. Ce processus nécessite néanmoins qu'une part significative des acteurs (utilisateurs et valideurs) accepte de basculer dans le nouveau système (les quelques cas existants ont montré que les acteurs ont tendance à se diviser, entre ceux de la chaîne historique et ceux de la nouvelle chaîne, en fonction de leurs intérêts propres).

Au-delà de ces propriétés intrinsèques, la question des performances est centrale dans la comparaison entre un système reposant sur une technologie de *blockchain* et les systèmes classiques. Très variables en fonction des technologies, ces performances sont en augmentation, notamment dans le cas des transactions financières : le temps de validation d'un bloc est de 10 à 20 minutes pour Bitcoin, de quelques minutes pour Ethereum, et de quelques secondes seulement pour les nouvelles crypto-monnaies. Par ailleurs, les technologies reposant sur les preuves de travail impliquent d'effectuer des quantités très importantes de calculs qui les rendent particulièrement peu efficaces en termes énergétiques.

Une multitude de services construits à partir des technologies disponibles

Les technologies construites autour de la *blockchain* se présentent comme des protocoles ou des plateformes à partir desquels il est possible de construire des services répondant à des cas d'usage. Certains services pourtant non financiers s'appuient même sur le Bitcoin, qui a été conçu au départ exclusivement pour réaliser des transactions monétaires. Il existe aujourd'hui des milliers de

(2) Il est néanmoins possible de trouver des solutions à cette limite grâce à des techniques permettant de manipuler les éléments sans en révéler le contenu, telles que le zero-knowledge protocol *(preuve à divulgation nulle de connaissance).*

services reposant sur des technologies construites autour du concept de *blockchain*, et de nouvelles variantes apparaissent régulièrement.

Les domaines d'application et les cas d'usage sont extrêmement variés : au-delà d'un secteur financier fortement mobilisé par le phénomène Bitcoin (210 milliards de dollars d'investissements estimés en 2016), des services existent dans l'énergie, le commerce (diamant ou œuvres d'art), les transports et la logistique, la gestion des droits numériques (musique, films ou jeux vidéo), la santé, l'administration et l'État (cadastre)… Le suivi de transactions, leur traçabilité ou la lutte antifraude sont les cas les plus répandus.

Le développement de ces services fait apparaître quatre enjeux principaux qui doivent être pris en compte afin d'évaluer l'adéquation entre un cas d'usage, un service et une technologie :

- la gouvernance : les règles d'organisation des communautés d'acteurs (utilisateurs ou valideurs) ainsi que leur mécanisme de régulation sont déterminants pour la pérennité du service ;
- l'efficacité technique : la comparaison avec les techniques classiques de bases de données réparties accessibles *via* des API est rarement en faveur des nouveaux services. Les performances des technologies de *blockchains* ne sauraient en être trop éloignées, sous peine d'échec ;
- la reprise de l'existant et la gestion des contentieux à venir (nombre de services ignorent cet enjeu) ;
- la numérisation des sous-jacents : certains services nécessitent que l'on associe de manière certaine des objets physiques (tels qu'un diamant, une toile ou l'énergie produite par une éolienne) à leur contrepartie numérique utilisée dans la chaîne correspondante. Cette question dépasse les seuls usages dans le cadre de la *blockchain*, mais cet écosystème a permis de développer plusieurs solutions d'efficacité apportant des degrés de garantie variables. Une réponse est l'utilisation d'« oracles » (également utilisables notamment pour les *smart contracts*), c'est-à-dire de tiers de confiance spécialisés choisis par les utilisateurs du service.

Un écosystème aux motivations variées

L'enthousiasme suscité par la *blockchain* et son potentiel d'applications ont entraîné la constitution rapide d'un écosystème riche. La *blockchain* figure en très bonne place dans le pic des espérances exagérées du « *Hype Cycle* » de Gartner [3] : c'est un signe d'effet de mode et de démultiplication des initiatives, mais également d'immaturité du domaine et d'apprentissage par l'expérimentation.

Plusieurs types d'acteur participent à l'écosystème de la *blockchain* :

- de nombreuses *start-ups* se sont lancées, y compris dans un rôle de conseil ;
- des tiers de confiance historiques (tels que les notaires, qui anticipent la mutation de leur métier) montent des expérimentations pour leurs propres usages ;
- de grands groupes, notamment dans le domaine financier (banques, assureurs…), l'expérimentent en partenariat avec des *start-ups* ou avec les acteurs du monde de la recherche et de l'innovation ;
- les pouvoirs publics, tant en France qu'à l'international (Caisse des Dépôts, France Stratégie, *UK Government Office for Science*) accompagnent ou observent le phénomène.

Les motivations des différents acteurs sont variées. La première d'entre elles est l'apprentissage : nombre d'initiatives visent principalement à tester des modèles techniques et organisationnels et à obtenir des retours d'expérience afin de mieux comprendre le concept de *blockchain* et les technologies associées, et de tenter de les maîtriser.

Par ailleurs, étant structurellement décentralisée, la *blockchain* entraîne l'apparition d'un effet de réseau : l'on assiste, de ce fait, à une course entre de nombreux acteurs désireux de devenir le service ou la plateforme de référence dans leur secteur et de s'assurer ainsi une position dominante (« *Winner takes all* »). Dans cette course prennent place aussi bien les tiers de confiance traditionnels que des entreprises clientes souhaitant se passer de ces intermédiaires ou de nouveaux entrants cherchant à modifier de fond en comble l'organisation d'un secteur. Enfin, un certain nombre de *start-ups* visent autant leur rachat par un grand groupe que le développement d'une activité propre.

Un élément de la transformation numérique

L'apparition de la *blockchain* correspond à une nouvelle approche, décentralisée, de l'informatique, dont les impacts réels n'apparaîtront qu'à long terme. Il est difficile de déterminer dans quelle mesure les comparaisons avec l'apparition des protocoles TCP/IP (*Transmission Control Protocol/Internet Protocol*), dans les années 1980, sont pertinentes. Néanmoins, en permettant d'aller au-delà de la simple dématérialisation des transactions et des contrats, la *blockchain* nous offre la possibilité de modifier la manière dont nous concevons la gestion de la confiance dans les relations humaines et au sein des organisations associées. Initiant la transformation numérique de secteurs complets, elle va bien au-delà d'une simple question technique.

L'apparition des *smart contracts* (contrats intelligents), en particulier, va modifier en profondeur les métiers du droit : le bitcoin, la première application de la *blockchain*, concerne les paiements, qui sont la forme la plus simple de contrat. Les métiers du droit ont notamment pour fonction de traduire en clauses juridiques et en contrats les intentions des parties. Au-delà de la simple dématérialisation des contrats, les *smart contracts* correspondent à la transformation numérique de cette activité : ils permettent de traduire en code informatique les intentions des par-

(3) www.gartner.com/technology/research/methodologies/hype-cycle.jsp

ties et d'obtenir l'exécution automatique du contrat ainsi constitué, illustrant le principe « *Code is law* ». Cela justifie l'intérêt que les professions juridiques manifestent à l'égard des *smart contracts*.

Même si la rédaction des *smart contracts* est un exercice complexe encore mal maîtrisé, et même si la gestion des contentieux reste une question ouverte, on peut s'attendre à voir se développer de nouvelles professions autour de la rédaction de *smart contracts* en lien avec plusieurs technologies de *blockchain*, ainsi que des échanges de bibliothèques de *smart contracts*. Là encore, les conséquences de la *blockchain* ne se cantonnent pas aux aspects techniques, elle a aussi des impacts juridiques et organisationnels. L'expérimentation est plus que jamais nécessaire pour comprendre ces nouveaux outils techniques et imaginer les nouvelles applications et les nouvelles formes d'organisation associées.

Les enjeux économiques de la *blockchain*

Par Patrick WAELBROECK
Professeur à Télécom ParisTech – Institut Mines-Télécom

La *blockchain* est une technologie qui va bien au-delà de l'horodatage, du bitcoin et de la sécurisation des transactions financières. Le développement d'un écosystème autour des objets connectés intelligents ne pourra sans doute pas se faire sans la *blockchain* (sous une forme ou sous une autre). La *blockchain* ouvre les portes de la liquéfaction du monde physique, de l'économie de la micro-transaction en temps réel et du partage intelligent de bases de données. Cependant, il est essentiel de distinguer les différents types de *blockchain*, en particulier les *blockchains* publiques des *blockchains* privées, car leurs propriétés économiques respectives sont très contrastées. Par ailleurs, les problèmes de gouvernance des *blockchains* publiques laissent à penser que la technologie *blockchain* ne pourra à elle seule assurer la confiance.

Introduction

La *blockchain* est une technologie. Elle correspond à un cahier sécurisé numérique décentralisé. Lorsqu'un nœud du réseau concerné veut enrichir ce registre d'un élément, tous les autres nœuds de la *blockchain* sont mis à contribution pour acter cet ajout de façon indélébile. Chaque bloc contient l'empreinte du bloc précédent, formant ainsi une chaîne de blocs de données. Une nouvelle entrée ne peut donc être ni falsifiée ni antidatée, car la *blockchain* est copiée sur l'ensemble des nœuds du réseau.

Nous discuterons *infra* les éléments disruptifs de la *blockchain*. En effet, il ne s'agit pas seulement d'un outil permettant de générer de la confiance en permettant de stocker des données sécurisées. Si les banques s'intéressent beaucoup à la *blockchain*, c'est aussi parce qu'il est possible d'y inscrire des transactions, ce qui ne coûtera alors que quelques centimes – contre quelques euros actuellement. La *blockchain* permet ainsi d'attester de manière irréfutable et datée le moment où a été effectuée une transaction : il s'agit d'une technologie d'horodatage généralisée. Un tel registre peut également servir à référencer des titres de propriété intellectuelle ou des données cadastrales. Certaines *blockchains,* comme la *blockchain* Ethereum, permettent d'exécuter un code sur les éléments de la *blockchain*. Ces codes appelés *smart contracts* ouvrent de nouvelles perspectives à l'Internet des objets.

Il existe principalement deux types de *blockchain* : les *blockchains* publiques et les *blockchains* privées. Elles diffèrent entre elles au travers des autorisations qui sont accordées aux nœuds du réseau. Dans le cas d'une *blockchain* publique, tous les nœuds sont autorisés à écrire dans celle-ci, et à y lire les données. À l'opposé, seul un petit nombre de nœuds sont autorisés à écrire dans une *blockchain* privée. Ainsi, les règles de validation pour ajouter un nouveau bloc diffèrent elles aussi. Par exemple, dans le cas de la *blockchain* publique Bitcoin, l'incitation à sécuriser les éléments de la *blockchain* est liée à l'obtention de bitcoins à travers deux mécanismes : un montant fixe par bloc miné et un montant variable lié aux frais de transaction du minage. Pour une *blockchain* privée, les incitations sont plutôt liées à la gouvernance de la *blockchain* (nous proposons *infra* une analyse économique des différents types de *blockchain*).

Quelles sont les autres raisons pour lesquelles un économiste devrait s'intéresser à la *blockchain* ? Il en existe au moins trois (que nous détaillerons dans la suite de cet article).

Premièrement, les *blockchains* offrent une perspective intéressante pour l'économie de la sécurité en créant un système décentralisé d'incitations à sécuriser un système informatique (nous présenterons les éléments d'analyse économique *infra*).

Deuxièmement, les *blockchains* et les *smart contracts* permettent de mettre en relation des agents de manière décentralisée, redéfinissant ainsi la notion d'entreprise et la nature du travail. Ils ont également un impact sur l'organisation des industries, puisque des agents peuvent partager des ressources informatiques, ce qui permet de réduire les coûts fixes d'entrée dans des secteurs qui nécessitent d'importants investissements dans des serveurs et du matériel informatique. Les *blockchains* représentent aussi un contrepoids aux tendances centrifuges des plateformes à plusieurs versants concentrant le pou-

voir de marché de certains acteurs de l'Internet (nous y reviendrons).

Nous proposerons de retenir le bitcoin comme objet d'une étude de cas présentée *infra*. Il s'agira pour nous, dans un premier temps, de mieux comprendre l'offre et la demande de cette crypto-monnaie. Nous ferons un détour important par la gouvernance du bitcoin, car les problèmes soulevés par celle-ci se posent également aux autres *blockchains*. Nous serons alors en mesure d'analyser la valeur économique du bitcoin.

Ensuite, la *blockchain* est également une innovation technologique qui peut se diffuser plus ou moins rapidement dans l'économie. Cette question fait actuellement l'objet d'un débat que nous présenterons dans la suite de l'article. Il s'agit de savoir si cette technologie est suffisamment disruptive pour connaître une diffusion très rapide ou si, au contraire, il s'agit d'une innovation transformative dont la diffusion complète dans le tissu économique pourrait nécessiter plusieurs décennies.

Quels sont les éléments disruptifs de la *blockchain* ?

La *blockchain* s'applique bien sûr aux produits numériques ou facilement numérisables. Mais la *blockchain* va bien au-delà de son utilisation comme simple registre numérique permettant un horodatage. Trois aspects méritent d'être soulignés : les *tokens,* les *smart contracts* et la liquéfaction du monde physique.

L'économie des *tokens*

La *blockchain* rémunère le travail de sécurisation au moyen de l'émission de jetons (*tokens*). Ceux-ci peuvent correspondre à de la crypto-monnaie, mais ils peuvent également être assimilés à des droits de vote. La valeur des *tokens* augmente avec le nombre de leurs utilisations possibles : ainsi, par exemple, il existe des externalités de réseaux positives directes et indirectes entre ceux qui possèdent des bitcoins et ceux qui les acceptent (nous y reviendrons *infra*). Les jetons peuvent également servir pour garantir des droits de vote lors d'une assemblée générale ou lors d'élections politiques.

Les *smart contracts*

Les *smart contracts* sont des bouts de code, qui, exécutés sur la *blockchain*, permettront de valider des tâches et les rémunérations liées.

Un premier exemple, celui d'Ubik. Dans le livre de Philip K. Dick (1969), Joe Chip, spécialiste de la traque des télépathes, habite dans un appartement loué. Il attend une visite et souhaite faire le ménage. Il appelle le service d'entretien de l'immeuble pour que celui-ci lui envoie des robots nettoyeurs. Tout le service de conciergerie est automatisé : le robot (ou le *chatbot*, dirait-on aujourd'hui) l'informe qu'il a une dette à éponger avant de pouvoir recruter les robots nettoyeurs. Comme il est sans le sou, il souhaite faire appel à un microcrédit en temps réel. Cependant, le robot l'informe également que la société de vente de crédits a abaissé sa note personnelle de crédit de triple G à quadruple G et bloque toute nouvelle demande de crédit. Il utilise une pièce de 10 *cents* pour mettre la cafetière en marche, mais il lui manque 5 *cents* pour pouvoir ouvrir la porte de son appartement pour faire entrer ses invités (qui finalement paient eux-mêmes pour ouvrir la porte). Il leur propose un café, mais le réfrigérateur est également automatisé et 10 *cents* sont nécessaires pour l'ouverture de la porte et 5 *cents* pour obtenir de la crème. Il s'agit d'une économie du micropaiement et de la microtransaction en temps réel (ici, l'emprunt bancaire). Cet univers économique a été présenté comme une alternative au *copyright* permettant de rémunérer les créateurs par Jason Lanier (2013). L'idée de la porte connectée d'Ubik est actuellement en développement chez Slock.it, qui réfléchit à une solution permettant de déverrouiller une porte sous condition de paiement.

Une liquéfaction du monde physique

La *blockchain* permet également de tracer et d'authentifier des personnes et des produits physiques grâce à des techniques d'empreinte, de reconnaissance numérique et à des capteurs. Il peut s'agir, par exemple, de tracer un numéro de série ou le « passeport » d'un objet physique dans la chaîne de production. Ces technologies font converger le monde physique avec le monde numérique en améliorant la traçabilité des produits et des services pour rendre l'économie plus « liquide ».

L'exemple d'un *daemon*. Un *daemon* est un programme informatique qui réside en mémoire et qui exécute des tâches lorsque certains événements se produisent. Il s'agit du prototype d'un *smart contract*, mais sans la dimension micropaiement. Daniel Suarez (2006) relate l'histoire d'un programmeur de jeux vidéo de génie, Matthew Sobol, qui orchestre après sa mort des exécutions automatiques sur des objets connectés : maison piégée, porte électrifiée, véhicule autoguidé tueur… Il ne s'agit pas vraiment d'intelligence artificielle, mais bien d'une exécution automatique conditionnelle distribuée. Le *daemon* auto-exécute des tâches grâce à des capteurs physiques qui lui permettent de détecter des événements réels. Il « suit » également les *news* sur Internet pour vérifier les séquences d'événements.

L'exemple d'Everledger. Everledger est une *blockchain* du diamant qui permet de tracer les transactions grâce à un système de passeport numérique attribué à chaque diamant. Les métadonnées de chaque diamant (sa taille, son diamètre, son poids, etc.) sont également enregistrées dans la *blockchain*.

Les propriétés économiques des *blockchains*

Les *blockchains* ont différentes caractéristiques économiques. Il est intéressant de les analyser en fonction des permissions de lecture et d'écriture, de rivalité et d'excluabilité, ainsi que d'externalités de réseau.

Les permissions d'écriture et de lecture

Il est important de distinguer les *blockchains* selon que l'on ait ou non besoin d'une permission pour y écrire des données et d'une permission pour en lire certaines des

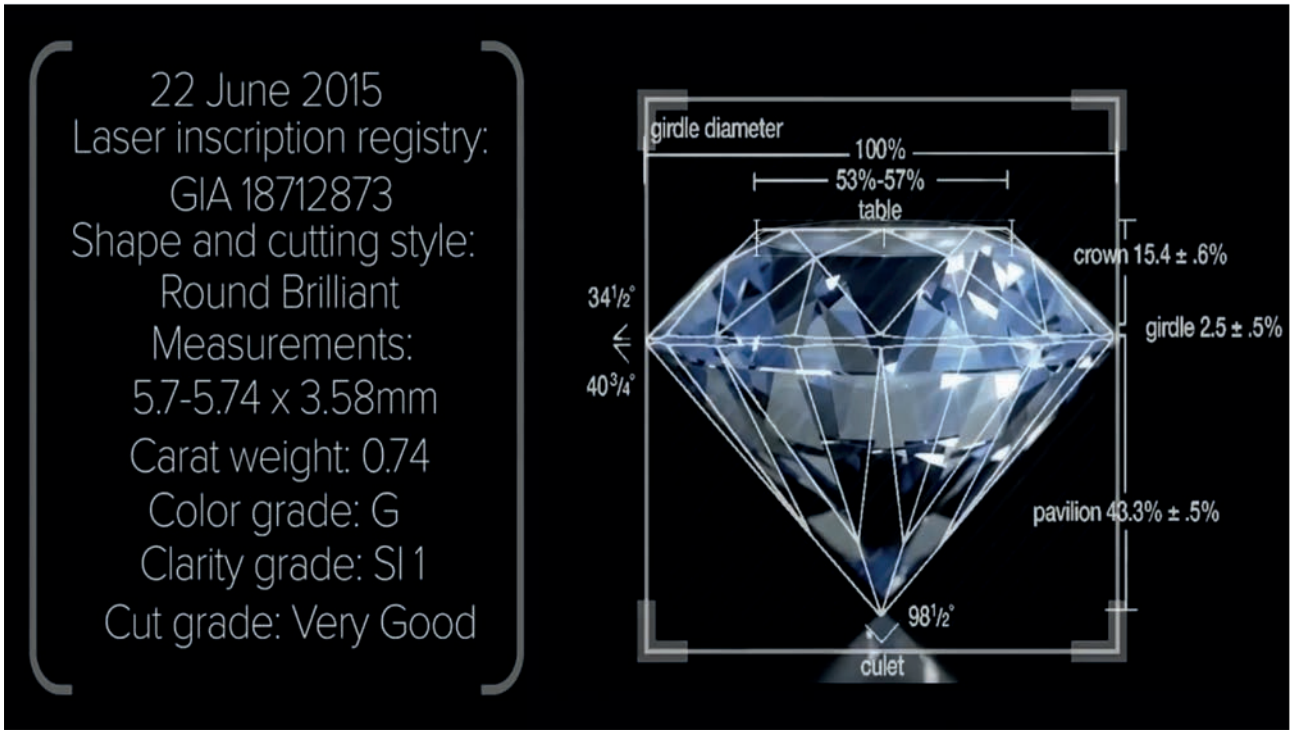


Figure 1 : Les spécifications quantitatives et qualitatives d'un diamant taillé répertorié dans la *blockchain* Everledger.
Source : https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/ (consulté le 17 mai 2017).

données. Les quatre configurations des permissions possibles sont représentées dans le Tableau 1 ci-dessous.

	Permission de lecture	Sans permission de lecture
Permission d'écriture	*Blockchain* privée	*Blockchain* gouvernementale
Sans permission d'écriture	Surveillance/assurance	*Blockchain* publique

Tableau 1 : *Blockchains* avec ou sans permission de lecture et/ou d'écriture.

Deux configurations sont généralement discutées par les experts du domaine.

Premièrement, les ***blockchains* privées** nécessitent à la fois une permission pour lire les données stockées et une permission pour y écrire. Elles se développent très rapidement, car leur gouvernance est aisée et la confidentialité des données y est relativement garantie, puisqu'un nombre limité d'acteurs peuvent y accéder. Ce nombre limité d'acteurs permet également de déterminer facilement les responsabilités en cas de problème. Ce sont typiquement les *blockchains* correspondant à un usage spécifique, comme la *blockchain* Everledger (que nous avons citée supra).

À l'opposé, **les *blockchains* publiques** sont ouvertes à tous, ce qui pose des problèmes de gouvernance et de responsabilité. Ce sont les premières *blockchains* de crypto-monnaies, telles que le bitcoin et l'éther. La confidentialité de leurs données est garantie par l'utilisation de pseudonymes. Néanmoins, toutes les transactions correspondant à un pseudonyme sont visibles par tous et peuvent être explorées grâce à des outils de recherche, tels que *blockchain.info*. Les deux autres configurations de permission sont beaucoup moins répandues, mais elles sont également en train d'être développées. Comme exemple de *blockchains* sans permission d'écriture, mais avec permission de lecture, on peut penser à certaines *blockchains* gouvernementales, telles que des registres cadastraux. Ainsi, l'État américain du Delaware développe actuellement une initiative avec la *start-up* Symbiont.io pour automatiser son processus d'*Initial Public Offering* (IPO) (introductions en bourse) grâce aux *smart contracts*. En ce qui concerne les *blockchains* sans permission d'écriture, mais avec permission de lecture, on peut penser également aux *blockchains* de compagnies d'assurance qui monitorent les événements grâce à des objets connectés et qui déclenchent des remboursements automatiques grâce aux *smart contracts,* si les conditions sont satisfaites.

Rivalité et excluabilité

On considère qu'en général, les biens économiques présentent deux caractéristiques : leur rivalité et leur excluabilité. Les données stockées dans une *blockchain* restent non rivales. En revanche, le mode de gouvernance de la *blockchain* permet, dans certains cas, de priver certains utilisateurs du droit de lecture et/ou d'écriture des données. On est donc soit dans le cas de biens non rivaux et excluables, à savoir des biens de clubs, ou dans le cas de biens non rivaux et non excluables, c'est-à-dire des biens collectifs.

Considérons maintenant les jetons générés par la *blockchain*. Ces jetons sont des biens rivaux, une seule personne pouvant utiliser un jeton donné. En revanche, on peut empêcher certaines personnes d'y accéder (*blockchain* privée), auquel cas l'on a affaire à un bien privé. Si tout le monde peut accéder à la ressource, comme

dans le cas des *blockchains* publiques, on est en présence de biens communs.

Externalités négatives et externalités positives liées aux investissements en minage

Dans le cas des *blockchains* nécessitant un minage pour valider de nouveaux blocs, il existe deux types d'externalités de réseau directes.

Premièrement, il existe des externalités de réseau positives liées à la sécurisation de la *blockchain*. Ces externalités de réseau positives surviennent lorsque la valeur du produit ou du service augmente avec le nombre d'utilisateurs. Par exemple, la valeur d'un certain type de logiciel augmente avec le nombre de ses utilisateurs, car il est plus facile d'échanger des fichiers avec des amis, avec des collègues et avec d'autres contacts. Dans le cas de la *blockchain*, chaque nœud supplémentaire en renforce la sécurité, car il est plus difficile de mener des attaques de type 51 % ou de deviner le gagnant du processus de minage (attaques DOS – *Denial Of Service*) (nous développerons ce point *infra*).

Cependant, il existe aussi une externalité négative : chaque mineur, lorsqu'il investit dans du nouveau matériel, augmente son revenu marginal, mais il augmente aussi le coût global du minage, car la difficulté augmente avec le nombre des mineurs et avec leurs capacités de calcul (*hash-power*). Par exemple, pour le réseau bitcoin, la difficulté du problème de cryptographie à résoudre est validée par un consensus de *proof-of-work* qui augmente avec le *hash-power* global du réseau. Il y a donc un risque de surinvestissement dans la capacité de minage, car les mineurs individuels ne prennent pas en compte l'effet négatif sur l'ensemble du réseau.

Il est important de souligner qu'augmenter la difficulté du minage réduit les incitations à miner et augmente le temps de vérification, et donc l'efficacité même de la *blockchain*. Ce mécanisme rappelle la tragédie des communs dont les ressources partagées (le *hash-power*) dépérissent et ne sont entretenues que par une poignée de fermes et de *pools*, annulant de ce fait le principe même de la *blockchain* publique, qui se veut décentralisée. Il y a donc un risque que les capacités de minage soient fortement concentrées entre les mains d'un petit nombre d'acteurs, rendant caduc le principe même de la *blockchain*.

Les *blockchains* privées résolvent les externalités négatives de minage, au risque de créer une tragédie des anti-communs, qui traduit l'idée qu'il n'y aurait plus de ressources communes, mais uniquement des ressources privées protégées par le droit de la propriété privée.

Les externalités de réseau indirectes

Les *blockchains* mettent souvent en relation plusieurs groupes d'agents. C'est le cas des crypto-monnaies, qui apparient acheteurs et commerçants, ainsi que des plateformes mettant en relation emprunteurs et prêteurs, ou encore vendeurs et acheteurs de diamants (pour reprendre l'exemple d'Everledger). Ces différents types de marché partagent la caractéristique des marchés à plusieurs versants dans lesquels deux ou plusieurs groupes d'agents se rencontrent. Sur ce type de marché, il existe des externalités de réseau indirectes, souvent positives : la valeur du service proposé par la plateforme pour un groupe d'agents augmente avec le nombre des agents de l'autre groupe. Ces marchés sont typiquement très fortement concentrés dans l'économie numérique. On pense à des plateformes telles que YouTube, Google, Facebook, eBay, etc. Il est intéressant de souligner que les *blockchains* publiques ne sont pas centralisées, elles sont au contraire fortement décentralisées (nous reviendrons sur ce point *infra*).

Les différences entre *blockchains* privées et *blockchains* publiques

Comparons maintenant les avantages et les inconvénients des *blockchains* privées à ceux des *blockchains* publiques. Si la *blockchain* publique représente une solution de confiance décentralisée pour beaucoup, la *blockchain* privée peut être complètement centralisée entre un petit nombre d'acteurs, prenant le contrepied du rêve libertaire de la *blockchain* publique. Il est donc important de distinguer ces deux types de *blockchain*, qui diffèrent énormément sur le plan de la gouvernance.

L'une des différences majeures entre *blockchain* privée et *blockchain* publique est liée à la confidentialité des *smart contracts*, des transactions et des données.

Comme nous l'avons souligné précédemment, il est relativement facile de garantir la confidentialité des données stockées dans des *blockchains* privées, puisque seul un nombre limité d'acteurs peut y avoir accès, ce qui explique leur développement rapide.

Les données stockées dans les *blockchains* publiques sont au contraire accessibles à tous, puisqu'il s'agit de construire un registre public décentralisé. Cela dit, il est possible d'obtenir certaines formes de confidentialité dans les *blockchains* publiques qui utilisent des pseudonymes (c'est le cas pour le réseau bitcoin). Par ailleurs, certaines solutions techniques sont développées sur des *blockchains* publiques pour protéger les données sensibles. Ainsi, le projet Enigma du MIT (*Massachusetts Institute of Technology*) propose une *blockchain* de données de santé dans laquelle un nœud du réseau ne peut accéder à l'ensemble des données en utilisant une infrastructure *Secure Multiplatform Computation* : ces données sont réparties sur les différents nœuds du réseau et ne peuvent pas être entièrement révélées dans leur intégralité lors d'une requête. D'autres initiatives sont basées sur une technique de *zero knowledge proof* qui permet de vérifier la validité de transactions dont les métadonnées sont cryptées.

Les *blockchains* privées et les *blockchains* publiques diffèrent également sur deux autres dimensions : l'efficacité de la preuve et la gouvernance.

Premièrement, le passage à l'échelle est difficile sur une *blockchain* publique utilisant un consensus basé sur le *proof-of-work* (comme celui utilisé par le réseau bitcoin), puisque celui-ci demande un *hash-power* qui croît avec la taille du réseau et nécessite plusieurs validations avant

l'ajout d'un nouveau bloc, ce qui peut prendre une heure. D'autres types de consensus sont étudiés, comme le *proof-of-stake*, sur le réseau Ethereum. Les *blockchains* privées utilisent des consensus qui permettent d'écrire un très grand nombre d'informations à la minute, comme dans le cas d'un consensus basé sur la *delegated proof-of-stake*.

Deuxièmement, la gouvernance d'une *blockchain* publique nécessite un accord de l'ensemble des nœuds du réseau pour valider un changement majeur du protocole de validation des données (nous développerons ce point important dans la suite de cet article). Une décision peut être prise par un très petit nombre de nœuds, dans le cas d'une *blockchain* privée.

Enfin, se pose la question ouverte de la responsabilité. Les spécialistes de la *blockchain* en France considèrent qu'il est beaucoup plus facile d'établir les responsabilités dans le cas d'une *blockchain* privée (en particulier si les contrats ressortissent d'un même droit national). Dans le cas d'une *blockchain* publique internationale, cette question fait l'objet d'analyses légales.

	Blockchains privées	*Blockchains* publiques
Gouvernance	+	-
Externalités indirectes (plateformes multi-versants)	0/+	+
Externalités de sécurité	0	+
Externalités négatives de minage	0	-
Efficacité de la preuve	+	-
Externalité de sécurisation	0	+
Responsabilité	+	-
Ouverture et interopérabilité	-	+
Confidentialité	+	0
Monétisation	+	0

Blockchains et économie de la sécurité

Nous allons étudier maintenant les facteurs qui peuvent influencer les décisions des entreprises en matière de sécurisation de leur infrastructure informatique. Nous montrerons dans un premier temps que les forces économiques poussent les entreprises à sous-investir en la matière. Nous analyserons ensuite en quoi la *blockchain* permet d'apporter des solutions aux enjeux économiques de la sécurité informatique.

Prenons l'exemple des données de clients. Tout d'abord, il existe des externalités négatives associées au manque de protection des données qui ne sont pas compensées par les mécanismes du marché. Cela peut conduire à des situations dans lesquelles les données des clients sont exposées à des fuites, à des fraudes ou à des vols. Ensuite, les entreprises développent des stratégies leur permettant d'atteindre rapidement une masse critique, au détriment de leur infrastructure de données. Enfin, l'asymétrie de l'information par rapport au niveau de sécurité de l'infrastructure de données permet aux entreprises de partager les données personnelles de leurs clients avec des tiers qui ne sont pas forcément inciter à les protéger.

Les biens publics

Les biens publics sont non rivaux et non excluables. Ces deux caractéristiques impliquent qu'un seul agent ne peut pas capturer le surplus total qu'il crée pour l'ensemble de la société. Il y aura donc sous-investissement de la part du secteur privé. De plus, dans un écosystème de sociétés partageant des données, les membres individuels bénéficient des efforts des autres membres qui sécurisent le système. Dans l'ensemble de l'écosystème, les données seront donc faiblement protégées.

Les externalités des réseaux

Moore et Anderson (2012) étudient l'effet des externalités du réseau sur le niveau de sécurité mis en œuvre par les fabricants de logiciels. Il est important pour une entreprise qui veut dominer un marché grâce à de fortes externalités de réseau positives d'atteindre rapidement la masse critique. Dans ce contexte, il existe très peu d'incitations à consacrer du temps et des efforts à la sécurisation des données personnelles. Au contraire, il est plus profitable de laisser d'autres trouver des *bugs* et des trous de sécurité, puis de résoudre ces problèmes au moyen de mises à jour et de correctifs logiciels.

Les modèles d'affaires basés sur des échanges de données

Lorsque les entreprises développent des stratégies commerciales basées sur la publicité, elles génèrent des revenus en vendant les données de leurs clients à des tiers. Ces entreprises sont incitées à rédiger des conditions de service très générales pour pouvoir utiliser (et réutiliser) de manière exhaustive les données de leurs clients. Lorsque les données personnelles sont transférées à des tiers, il est vraiment difficile pour le client de déterminer comment ses données sont utilisées, stockées et sécurisées. Les ventes aux enchères en temps réel de données sur les *ad exchanges* exacerbent ces problèmes, car les données personnelles disponibles dans les *cookies* sont transmises et appariées par d'autres plateformes ou/et des sociétés tierces.

Les solutions apportées par la *blockchain*

La *blockchain* apporte des solutions aux problèmes de l'économie de la sécurité en incitant explicitement à la sécurisation. Dans le cas de la *proof-of-work* du réseau bitcoin, les incitations sont directement monétaires sous la forme de gains en crypto-monnaie. Dans le cas du *proof-of-stake*, la sécurisation permet de s'engager davantage dans la gouvernance de la *blockchain* et d'obtenir des parts dans les droits de vote. La gouvernance des *blockchains* permet également aux nœuds du réseau de se coordonner afin de contrer des attaques (voir BÖHME *et al*., 2015).

Malgré ces objectifs atteints en termes d'incitations, l'algorithme de *hash* du bitcoin est basé sur une technologie SHA-256 (*Secure Hash Algorithm*) qui risque de devenir obsolète. Par ailleurs, contrairement à la terminologie utilisée, les *smart contracts* ne sont que des bouts de code, qui peuvent contenir des *bugs*, comme tout programme informatique. On peut mentionner à cet égard le *smart contract* DAO, sur le réseau Ethereum, qui contenait un *bug* qui a permis à un groupe de *hackers* de subtiliser 50 millions de dollars. Enfin, les données sont protégées par une clé privée qui, si elle est perdue, empêche l'ac-

cès aux données stockées, mais qui, si elle est extorquée, compromet la sécurité des données.

Blockchains, nature de la firme et économie industrielle

La *blockchain* n'a pas seulement un impact sur l'économie de la sécurité. Elle peut remettre en question la définition même de l'entreprise, du travail et de l'organisation des industries numériques. Chaque industrie du numérique est aujourd'hui dominée par une entreprise en situation de quasi-monopole. Cette situation résulte principalement de deux forces économiques : premièrement, les investissements réalisés par les entreprises en place dans le matériel et l'infrastructure génèrent des coûts fixes de production et d'entrée sur le marché qui créent eux-mêmes des rendements d'échelle croissants ; deuxièmement, les externalités de réseau positives directes et indirectes présentes sur les plateformes à plusieurs versants créent une force centrifuge générant un « effet boule de neige ». Ces deux forces sont remises en question par la *blockchain*.

Smart contracts et *Dencentralized Autonomous Organizations*

La *blockchain* permet un système de vote décentralisé. Cela peut remettre en question le rôle même des structures hiérarchiques, dans lesquelles les décisions des travailleurs se situant au bas de l'échelle hiérarchique sont déléguées à un supérieur, en remontant successivement jusqu'au PDG. Grâce au système de vote permis par la *blockchain*, tous ces travailleurs pourraient, en principe, prendre eux-mêmes les décisions stratégiques. En poussant le raisonnement à l'extrême, on pourrait même se passer de PDG...

Il est souvent accepté, après les travaux de R. Coase (1937), que la taille de l'entreprise est déterminée par les coûts de transaction pour effectuer une tâche en interne ou en externe. La *blockchain* permet d'étendre les relations contractuelles à des fournisseurs et à des travailleurs à plus faible coût. En poussant le raisonnement plus loin, la *blockchain* a deux conséquences sur l'entreprise et le travail salarié. Premièrement, la notion d'entreprise est elle-même menacée : une industrie serait alors organisée autour d'une *blockchain* et de *smart contracts* conclus entre différentes unités de tailles relativement petites. Deuxièmement, le travail salarié serait également remplacé par du travail indépendant. Cette tendance est déjà visible sur des plateformes centralisées comme Uber, mais elle n'est pas contredite par l'avènement de solutions décentralisées comme les *blockchains*.

Entrée sur le marché et contestabilité

Si les coûts fixes liés à l'infrastructure informatique et matérielle découragent l'entrée sur le marché, la *blockchain* permet à des agents indépendants de mettre leurs ressources en commun pour exécuter des tâches automatisées. Les marchés redeviennent contestables et l'entrée de nouveaux consortiums pourrait représenter un défi pour les entreprises existantes (même pour celles disposant d'un quasi-monopole).

Décentralisation des marchés

Enfin, la *blockchain*, à travers la décentralisation des tâches et du travail, est à contre-courant de plateformes telles qu'Uber ou Airbnb. Reprenons l'exemple d'Ubik et de la porte intelligente : de fait, tout objet doté d'un verrou intelligent permet, par exemple, d'automatiser une location, de sécuriser des armes ou de gérer des coffres-forts. Cependant, même si certains observateurs avancent l'idée que la *blockchain* pourrait finir par « ubériser Uber », rien n'est moins sûr. En effet, Uber pourrait également développer sa propre *blockchain* pour automatiser ses contrats avec les chauffeurs. De la même manière, Airbnb pourrait développer sa *blockchain* pour automatiser le paiement des locations et de la conciergerie.

Étude de cas : l'exemple emblématique du bitcoin

Le réseau bitcoin est le premier réseau *blockchain* public à s'être développé de manière massive. On comptait, en mai 2017, près de 7 000 nœuds sur ce réseau. Chacun de ces nœuds peut cacher des *pools* (des ressources partagées) et des fermes de plusieurs milliers d'unités ASIC (*Application Specific Integrated Circuit*) développées pour miner les blocs. Les principaux *pools* et fermes sont localisés en Chine.

Le consensus basé sur le *proof-of-work* prévoit une augmentation de la difficulté du problème cryptologique à résoudre en fonction du *hash-power* global du réseau. Ainsi se pose, dans un premier temps, la question du coût de la *blockchain* publique. Le second point que nous aborderons sera celui de la gouvernance. Enfin, nous terminerons sur la valeur économique du bitcoin.

Le coût de la *blockchain* bitcoin

L'électricité représente la principale composante (entre 90 % et 95 %) du coût total d'une ferme de minage.

En 2015, Böhme *et al* (2015) évaluaient la consommation du réseau bitcoin à plus de 173 mégawatts d'électricité de manière continue. Cela représentait environ 20 % de la production d'une centrale nucléaire et un montant de 178 millions de dollars annuellement (au prix de l'électricité résidentielle aux États-Unis). Ce montant peut paraître important, mais Pierre Noizat estime que ce n'est pas plus que le coût annuel en électricité d'un réseau de DAB (distributeurs automatiques de billets) mondial, évalué à 400 mégawatts (http://e-ducat.fr/2015-11-28-cop21-et-blockchain/).

La gouvernance

La question de la gouvernance est cruciale pour comprendre le futur des crypto-monnaies. En effet, en cas de désaccord sur l'évolution du protocole de communication, le réseau risque de se diviser en plusieurs réseaux (*hard fork*) avec des monnaies incompatibles entre elles. La question la plus importante est liée au choix de la règle de consensus pour la validation de nouveaux blocs. Il faut parvenir à un consensus sur le consensus, ce que la technologie seule ne semble pas pouvoir fournir.

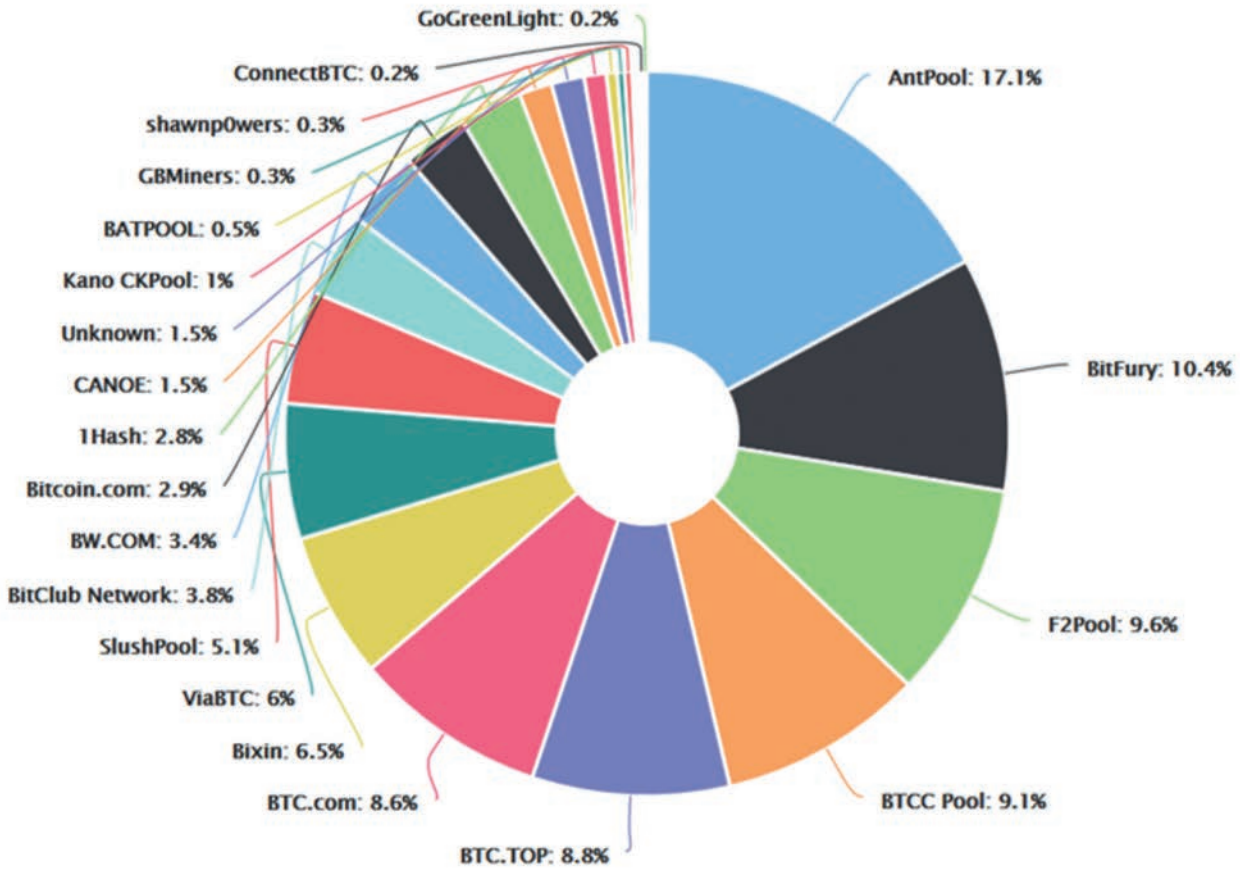


Figure 2 : Les partenaires *blockchain* du bitcoin.
Source : blockchain.info (consultée le 22 mai 2017).

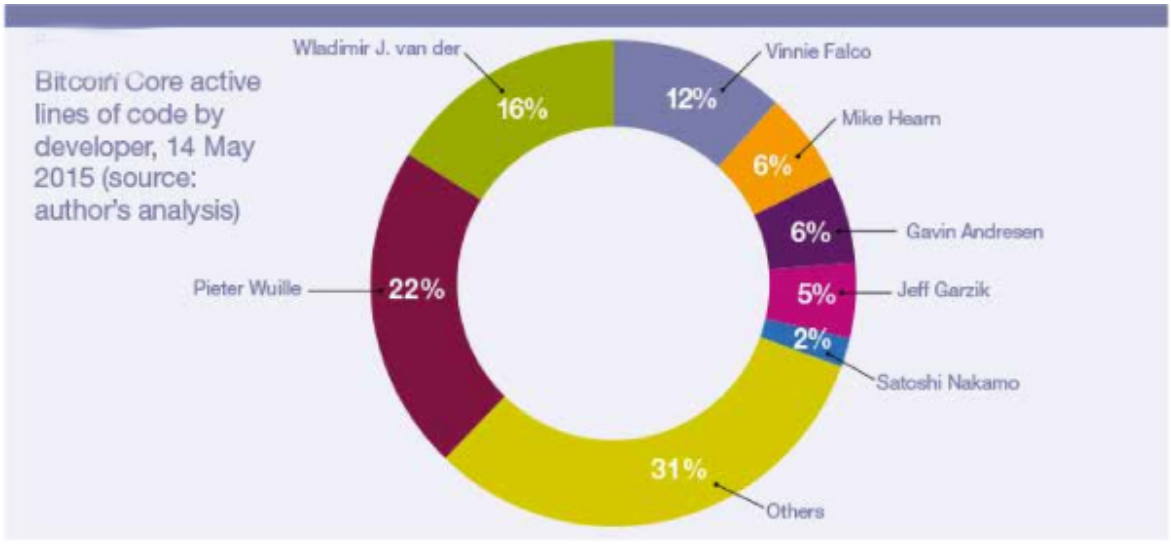


Figure 3 : Les principaux codes régissant le bitcoin et leurs développeurs (en mai 2015).
Source : WALPORT M. (2016).

Il faut noter que la répartition des *pools* indique clairement que le *hash-power* est concentré entre les mains d'une dizaine de *pools*, qui ont donc un pouvoir important lors de processus de décision en matière de changement des règles du protocole. Un protocole est l'équivalent de la grammaire pour une langue parlée. On peut ajouter ou retirer des règles, mais c'est au risque que les personnes ne se comprennent plus. Dans le cas du réseau bitcoin, on parle de *soft fork* et de *hard fork* lorsque l'on veut qualifier ces changements dans les règles.

Il existe plusieurs implémentations du protocole bitcoin : *bitcoin Core*, *Libbitcoin*, *bitcoin* XT, *bitcoin Classic*. Toutes ces implémentations sont globalement gouvernées par les core-développeurs. Par exemple, *Bitcoin Core* est gouvernée par un processus méritocratique d'évaluation par les pairs à travers un processus *Bitcoin Improvement Proposal* modéré par Wladimir Van Der Laan, lequel contribue de manière significative au codage du protocole bitcoin.

La gouvernance du protocole bitcoin est, quant à elle, décidée par les nœuds qui décident d'adopter tel ou tel changement d'implémentation. Le changement de protocole peut toucher les quatre couches du réseau bitcoin : la règle de consensus, la couche P2P, l'API (*Application Programming Interface*) et les applications (par souci de brièveté, nous ne discuterons que de la règle de consensus).

Pour ajouter une règle *soft fork*, une majorité de 95 % du *hash-power* est nécessaire ; les anciens blocs deviennent invalides et les nœuds *non upgradés* perdent en sécurité et en efficacité (*hash-power*). Pour forcer les mineurs à respecter les utilisateurs, une *soft fork* pourrait rendre le matériel de minage obsolète à travers un nouvel algorithme de minage. Pour retirer une règle *hard fork*, il est nécessaire que tous les nœuds complets adoptent le changement, sinon il y a un risque de voir le réseau bitcoin se diviser en deux réseaux non compatibles entre eux.

En conclusion, la technologie seule ne peut assurer la gouvernance. Il s'agit d'une situation paradoxale, dans la mesure où la technologie permet la décentralisation des vérifications et des exécutions automatiques, mais elle ne peut en garantir la gouvernance.

La valeur du bitcoin

Une crypto-monnaie n'a de valeur que si elle est considérée comme une monnaie par l'ensemble des participants au système monétaire. Elle nécessite donc d'être rare, au sens où elle ne peut pas être facilement copiée (problème équivalent à celui des faux billets, pour les monnaies traditionnelles). Cette propriété est satisfaite par le réseau *blockchain*, qui garantit l'absence de double dépense. En plus de cette valeur liée à l'acceptation, le bitcoin a de la valeur au travers de différents mécanismes économiques qui ne sont pas exclusivement monétaires. Nous les regrouperons à travers l'analyse de la demande et de l'offre de bitcoins. Nous commencerons par l'analyse des externalités de réseau et nous conclurons par une remarque sur le rôle joué par les monnaies alternatives dans un système monétaire.

Les externalités de réseau liées à la sécurité

Premièrement, le niveau de sécurité augmente avec le nombre des nœuds du réseau, car il faut d'autant plus de puissance de calcul pour compromettre la sécurité de la *blockchain* (à travers une attaque 51 %, *double spending* ou DOS). Par ailleurs, une attaque DOS est d'autant plus difficile à mener qu'il est difficile de deviner qui en est le bénéficiaire. Il existe donc des externalités de réseaux positives : la valeur du bitcoin augmente avec le nombre des nœuds participant au réseau.

Externalités de réseau indirectes positives liées au moyen de paiement

Le bitcoin est un moyen de paiement, au même titre que les espèces, les cartes bancaires ou les cartes Visa/Mastercard/American Express. Le bitcoin peut donc être appréhendé par la théorie des marchés à plusieurs versants qui modélise des situations dans lesquelles deux groupes d'agents économiques bénéficient d'externalités croisées. En effet, quand un consommateur choisit un moyen de paiement, il sera d'autant plus satisfait que ce dernier est accepté par le commerçant avec lequel il effectue une transaction. À l'inverse, pour un marchand, il est d'autant plus intéressant de proposer un moyen de paiement qu'il y a de clients qui le possèdent. Dès lors, la dynamique des marchés à plusieurs versants se traduit par des cycles vertueux qui peuvent connaître une phase d'amorce lente suivie d'une phase de déploiement très rapide. Si le bitcoin devait connaître une telle phase, sa valeur entrerait dans une phase d'accélération.

Par ailleurs, la commission payée par le consommateur ou le commerçant n'est pas contrôlée par une plateforme servant d'intermédiaire, mais par les mineurs (nous reprenons ce point dans la section suivante).

L'émission de monnaie sur le marché primaire

La création monétaire est divisée par 2 tous les 210 000 blocs pour arriver à un total de bitcoins en circulation (hormis ceux perdus) de 21 millions. Cette règle monétaire est contrôlée par le protocole bitcoin modifiable par le consortium *Bitcoin Foundation*, comme nous l'avons vu. La règle monétaire peut donc être modifiée pour répondre à des conditions de marché fluctuantes, au risque d'un *hard fork*. Par ailleurs, à demande constante, cette tendance à la baisse de l'offre de nouveaux bitcoins augmente automatiquement le prix du bitcoin. À terme, l'offre devenant inélastique, le prix du bitcoin (hors considérations spéculatives) est essentiellement déterminé par la demande.

La demande de crypto-monnaie

La demande de crypto-monnaie est issue de plusieurs préoccupations. Elle est également affectée par les incertitudes pesant sur sa pérennité.

Financial privacy

Les gouvernements limitent de plus en plus l'utilisation des espèces pour afficher leur lutte contre le blanchiment d'argent et le développement des marchés au noir. Le

cash est le seul moyen de paiement 100 % anonyme. Le bitcoin et les autres crypto-monnaies arrivent en deuxième position. En effet, le système de pseudonymat utilisé par le protocole bitcoin permet de masquer l'identité des personnes effectuant des transactions. Ainsi, certaines cryptomonnaies, comme le Zcash, masquent toutes les métadonnées d'une transaction.

Pourquoi utiliser un moyen de paiement anonyme ? Il existe de nombreuses raisons. Premièrement, l'utilisation d'un moyen de paiement anonyme permet d'éviter de laisser des traces qui peuvent être utilisées à des fins de surveillance par l'État, les employeurs et certaines entreprises (en particulier, les banques et les compagnies d'assurance). Ainsi, les entreprises et les banques pratiquent des stratégies de discrimination par les prix qui peuvent parfois se retourner contre les consommateurs. Laisser des traces par le paiement peut également pousser les entreprises à solliciter davantage les clients sur de nouvelles offres commerciales et la diffusion de publicités ciblées qui peuvent être considérées comme des nuisances par certains. Deuxièmement, payer avec un moyen de paiement anonyme limite également la sousveillance (ou surveillance inverse) par les proches. Ce sera le cas pour un paiement effectué à partir d'un compte commun. L'anonymat permet de limiter les externalités liées aux traces laissées lors d'un achat, il a donc une valeur économique. Le bitcoin, en permettant le pseudonymat, génère aussi de la valeur par ce biais.

Le bitcoin fonctionne en périodes de crise et permet donc d'éviter le contrôle des capitaux

Le bitcoin est apparu juste après la crise financière de 2008. Cette période a témoigné du pouvoir des gouvernements et des banques centrales en matière de contrôle des retraits d'espèces et du capital en circulation. Il n'existe que très peu de moyens d'échapper à ces deux contraintes institutionnelles. Le bitcoin en est un. En effet, même si les retraits d'espèces sont interdits, les possesseurs de bitcoins peuvent toujours payer en utilisant leur clé privée.

Les risques

Parmi les facteurs réduisant la demande de bitcoins, les risques liés à la réglementation et à la régulation ressortent tout particulièrement. D'une part, un État pourrait demander à ce que soient déclarées les plus-values générées par l'achat et la vente de bitcoins. Par ailleurs, les bitcoins peuvent être utilisés dans des secteurs réglementés (comme l'assurance ou la banque) et leur utilisation pourrait de ce fait également être réglementée. Enfin, il existe toujours le risque de perdre les données du disque dur sur lequel la clé privée est stockée, et donc de perdre les bitcoins associés, ou encore qu'un État impose son accès aux clés privées pour une question de sécurité.

La valeur du bitcoin sur le marché secondaire

Le bitcoin peut également être acheté et vendu sur une plateforme d'échanges. La valeur du bitcoin est alors plus proche de celle d'un investissement financier dont les acteurs anticipent les perspectives de gains et certains facteurs pouvant entraîner une appréciation du bitcoin.

Le bitcoin permet de discipliner les gouvernements

Le bitcoin (il en va de même pour les autres crypto-monnaies) peut être considéré comme une monnaie alternative non contrôlée par une banque centrale. Certains économistes, comme F. Hayek, considèrent que ces monnaies alternatives qui concurrencent la monnaie officielle permettent de discipliner les gouvernements qui seraient tentés de financer leur dette par l'inflation. Dans ce cas de figure, les consommateurs et les investisseurs se détourneraient de la monnaie officielle pour acheter la monnaie alternative et créeraient ainsi une pression déflationniste sur la monnaie officielle.

Perspectives économiques

La *blockchain* est inéluctable, car elle seule permettra le développement de l'Internet des objets. Cependant, la vitesse à laquelle cette transformation aura lieu est l'objet de débats entre spécialistes. Deux visions s'opposent : la vision de ceux qui pensent que la technologie prendra

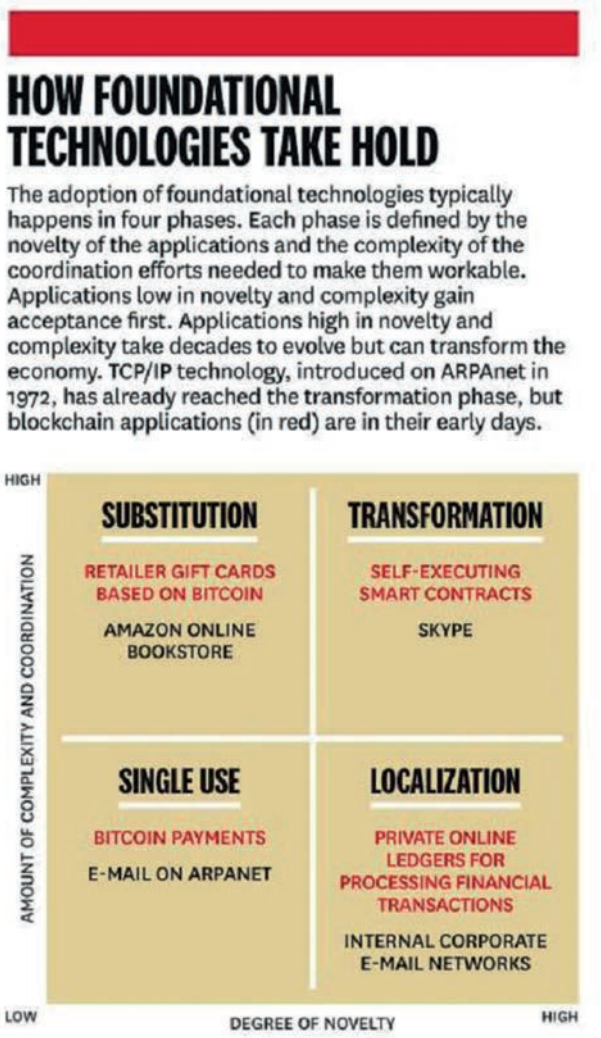


Figure 4 : Les quatre phases de l'adoption des technologies fondamentales : substitution, transformation, à des fins d'utilisation individuelle, à des fins de localisation (exemples illustratifs d'applications et de serveurs).
Source : LANSITI et LAKHANI (2017).

des décennies pour se diffuser et se transformer dans le tissu industriel, et la vision de ceux qui pensent qu'il s'agit d'une technologie disruptive.

La *blockchain* : est-elle transformative…

Lansiti et Lakhnani (2017) ont récemment suggéré que l'on pouvait établir un parallèle entre la diffusion d'une technologie transformative comme le protocole TCP/IP et la diffusion de la *blockchain*. Dans les deux cas, cette diffusion s'effectue en quatre phases qui peuvent prendre des décennies pour parvenir à la dernière, à savoir la phase transformative.

… ou disruptive ?

Au contraire, les spécialistes d'IBM voient dans la *blockchain* une technologie disruptive aux applications multiples allant de la logistique aux transactions financières.

Vectors of disruption	Liquification of the physical world
Unlock excess capacity of physical assets	Instantly search, use and pay for available physical assets
Create liquid, transparent marketplaces	Real-time matching of supply and demand for physical goods and services
Enable radical re-pricing of credit and risk	Digitally manage risk and assess credit, virtually repossess and reduce moral hazard
Improve operational efficiency	Allow unsupervised usage of systems and devices, reduce transaction and marketing costs
Digitally integrate value chains	Enable business partners to optimize in real-time, crowdsource and collaborate

Figure 5 : Cinq facteurs de disruption (1 – contre la puissance excessive des avoirs physiques ; 2 – en faveur de marchés plus liquides et transparents ; 3 – permettant une réévaluation drastique du crédit et du risque ; 4 – améliorant l'efficience opérationnelle ; et 5 – intégrant digitalement les chaînes de valeur) et leurs effets en termes de liquéfaction du monde physique.
Source : PURESWARAN et BRODY (2014).

Analyse

En première analyse, le protocole TCP/IP est à la fois similaire à la *blockchain* d'un certain point de vue et différent d'un autre. En effet, le protocole TCP/IP est un protocole ouvert, tout comme l'est la *blockchain* publique. En revanche, le protocole TCP/IP était au départ une affaire de spécialistes, alors que le bitcoin et la deuxième génération de la *blockchain* ont été très rapidement adoptés par des millions d'utilisateurs. Au final, la *blockchain* représente plus une technologie disruptive vouée à être adoptée massivement, qu'une technologie à diffusion lente. Mais il reste des verrous, qu'il est nécessaire de faire sauter (que nous présentons dans notre conclusion, ci-dessous).

Conclusion

En conclusion, la *blockchain* est une technologie révolutionnaire qui n'est pas limitée exclusivement au bitcoin. Le développement d'un écosystème autour des objets connectés intelligents ne pourra sans doute pas se faire sans la *blockchain* (sous une forme ou sous une autre). La *blockchain* ouvre les portes de la liquéfaction du monde physique, de l'économie de la micro-transaction en temps réel et du partage intelligent de bases de données. Cependant, un certain nombre de verrous doivent encore sauter. Premièrement, il s'agit d'établir clairement les responsabilités et le droit applicable aux *blockchains* publiques. Deuxièmement, il faudra garantir en Europe l'application de la protection des données personnelles (*General Data Protection Regulation* – GDPR). Troisièmement, il faudra déterminer le statut fiscal et juridique des crypto-monnaies. Enfin, quatrièmement, il faudra réfléchir à la manière d'articuler les *smart data* issues des *blockchains* avec le principe de neutralité du *Net* en Europe.

Bibliographie

BÖHME R., CHRISTIN N., EDELMAN B. & MOORE T. (2015), "Bitcoin: Economics, technology, and governance", *The Journal of Economic Perspectives* 29(2), pp. 213-238.

BRODY P. & PURESWARAN V. (2014), *Device democracy: Saving the future of the internet of things*, IBM, September.

COASE R. H. (1937), *The Nature of the Firm*, Economica 4(16), pp. 386-405.

DICK P. K. (1969), *Ubik,* trad. Alain Domrémieux (1999), Éditions 10/18.

LANIER J. (2013), *Who Owns the Future?*, Simon & Schuster.

LANSITI M. & LAKHANI K. R. (2017), *The truth about blockchain*, Harvard Business Review 95(1), pp. 119-127.

MOORE T. & ANDERSON R. (2012), *Internet security, The Oxford Handbook of the Digital Economy,* Oxford University Press.

SUAREZ D. (2006), *Daemon,* Verdugo Press.

WALPORT M. (2016), *Distributed Ledger Technology: Beyond Blockchain,* UK Government Office for Science.

La *blockchain* – Les défis de son implémentation

Par Ilarion PAVEL
Ingénieur en chef des mines, Conseil général de l'économie, de l'industrie, de l'énergie et des technologies et Laboratoire de physique théorique de l'École normale supérieure

Nous passerons en revue dans cet article plusieurs des difficultés techniques et défis juridiques, sociétaux ou réglementaires rencontrés dans l'implémentation de la *blockchain,* et nous suggérerons quelques pistes de solutions.

Introduction

La *blockchain* est apparue en 2008 comme partie intégrante du bitcoin [1], crypto-monnaie et système de paiement [2] qui fonctionne sans autorité centrale sur un réseau pair-à-pair, *via* des transactions cryptées. Toutes les transactions sont vérifiées par les nœuds du réseau et enregistrées dans un registre public réputé infalsifiable appelé *blockchain* [3].

Disposant de puissants moyens de calcul, certains nœuds du réseau qualifiés de « mineurs » vérifient, enregistrent et sécurisent les transactions. Celles-ci sont groupées dans des blocs, qui seront ensuite « enchaînés » l'un à la suite de l'autre pour former la *blockchain*. Le dernier bloc en date est ajouté au précédent (celui-ci étant dit « miné ») par le premier « mineur » qui réussit à résoudre un problème cryptographique difficile appelé « preuve de travail ». Ce mineur reçoit alors une certaine somme de bitcoins en récompense de sa réussite, et le nouveau bloc se propage à l'ensemble des nœuds du réseau.

Comme pour toute autre monnaie, on peut échanger des bitcoins contre de la monnaie fiduciaire, des produits ou des services en effectuant des transactions électroniques au moyen d'un logiciel installé sur un ordinateur personnel ou sur un terminal mobile, ou *via* une application *Web* [4].

Dès son lancement, le bitcoin a été imité par des systèmes de crypto-monnaies alternatives (*altcoins*) qui utilisent les mêmes techniques, mais avec diverses optimisations. De même, les techniques de la *blockchain* ont été utilisées, avec succès, pour mettre en œuvre des chaînes alternatives (*altchains*) qui permettent des applications autres que la monnaie électronique (gestion de ressources ou contrats), élargissant ainsi la sphère de la *blockchain*, qui était à l'origine consacrée exclusivement aux transactions financières. Il existe déjà quelques centaines d'*altcoins* et d'*altchains*, et ceux-ci sont en plein développement.

On appelle *blockchain* 1.0 tout ce qui concerne la monnaie électronique et ses opérations (émission, transfert, paiement), *blockchain* 2.0 l'ensemble des applications financières et économiques autres que celles liées à la monnaie (actions, obligations, contrats à terme, prêts, hypothèques, propriété intellectuelle, contrats intelligents) et *blockchain* 3.0 d'autres applications en dehors des sphères financière et économique (administration, santé, science, culture, art).

Le bitcoin est actuellement la monnaie cryptographique la plus utilisée dans le monde, avec un volume de transactions en pleine croissance [5]. Le bitcoin et ses alternatives (*altcoin, altchain*) vont probablement transformer le paysage financier et économique, mais leur implémentation risque de se heurter à plusieurs difficultés techniques, ainsi qu'à des défis de nature réglementaire, juridique et sociétale.

Les difficultés techniques

L'insuffisance de la capacité de transaction

La taille d'un bloc du bitcoin a été intentionnellement limitée à 1 Mo afin d'éviter des attaques du type « déni de service » : une personne mal intentionnée pourrait créer des blocs de grande taille et les diffuser à travers le réseau afin de provoquer des congestions, voire la paralysie du trafic.

Par ailleurs, le temps nécessaire pour miner un bloc a été fixé à environ 10 minutes. La diminution de ce laps

(1) NAKAMOTO (Satoshi), "Bitcoin: A Peer-to-Peer Electronic Cash System", https ://bitcoin.org/bitcoin.pdf
(2) Par abus de langage, on associe le terme « bitcoin » à la fois à l'unité de valeur de monnaie électronique, à la technologie sous-jacente et au réseau sur lequel cette dernière opère.
(3) De même, le terme « blockchain *» est utilisé à la fois pour désigner le registre, la technologie ou le réseau.*
(4) Les aspects techniques de la technologie bitcoin sont bien plus complexes. Il existe de nombreuses références : voir, par exemple, ANTONOPOULOS (Andreas) (2015), Mastering Bitcoin*, O'Reilly Media.*
(5) Pour des statistiques concernant le bitcoin, voir https://blockchain.info/

de temps augmenterait la fréquence du phénomène dit de « fourche » [6]. Or, plus un réseau présente des phénomènes de fourche, et plus il est vulnérable aux attaques, notamment du type 51 % qui sera décrit plus bas.

Autre effet de l'augmentation de la taille du bloc et de la diminution du délai séparant deux blocs : l'augmentation du nombre des blocs « orphelins » (minés mais point attachés à la *blockchain* [7]).

La conséquence de ces limites (taille du bloc, temps entre deux blocs) est que le bitcoin peut supporter seulement 7 transactions par seconde (tps), ce qui est bien plus faible que d'autres réseaux comme celui de la carte Visa, qui supporte 2 000 tps en moyenne, avec une capacité de surcharge ponctuelle pouvant aller jusqu'à 56 000 tps.

À terme, avec l'accroissement du nombre des transactions, le temps nécessaire à leur validation risque d'augmenter, ce qui augmentera les frais de transaction [8].

Des solutions possibles sont l'augmentation de la taille du bloc (la doubler, voire l'augmenter encore davantage), la réduction du temps entre deux blocs et la réduction du temps de latence (laquelle réduira le phénomène de fourche [9]). Ainsi, l'*altcoin* Litecoin fonctionne avec un temps entre deux blocs de 2,5 minutes, l'*altchain* Ethereum avec 17 secondes. On peut envisager des solutions plus radicales, comme la reconception du protocole bitcoin [10], mais cela demanderait un consensus entre les acteurs (notamment de la part des mineurs).

Enfin, une autre possibilité pourrait consister à construire des piles protocolaires de niveau supérieur, au-dessus du protocole bitcoin, sous la forme de contrats intelligents. Ces piles protocolaires permettraient des millions de transactions par seconde, grâce à des canaux de paiement dont seules l'ouverture et la fermeture seraient incluses dans la *blockchain* (comme c'est le cas dans les réseaux Lightning [11] et TumbleBit [12]).

Un temps de latence trop long

Le temps de latence est le temps nécessaire pour propager un bloc à partir d'un nœud du réseau vers l'ensemble des utilisateurs : il est en moyenne de 12 secondes. Après 40 secondes, en moyenne 95 % des nœuds du réseau reçoivent le bloc [13]. C'est long par rapport au réseau Visa, dont le temps de latence est de quelques secondes, et encore plus long si l'on envisage d'utiliser la *blockchain* pour sécuriser les applications pour l'Internet des objets, qui sera composé d'objets communicants en interaction permanente quasi instantanée.

La diminution du temps de latence nécessite également de modifier le protocole bitcoin ou d'ajouter des couches protocolaires de niveau supérieur.

La taille de la *blockchain*

La taille de la *blockchain* du bitcoin est actuellement de 115 Go, elle est en croissance rapide : elle a augmenté de 50 Go sur les douze derniers mois. Charger la *blockchain* sur un ordinateur demande actuellement plusieurs jours et suppose que l'on dispose de suffisamment de mémoire libre sur son disque dur [14]. Il est cependant probable que l'évolution future des performances des ordinateurs et du débit Internet permettra de faire face à l'augmentation de la taille des *blockchains*.

De plus, les utilisateurs peuvent choisir entre être un nœud complet (contenant toute la *blockchain*, ceux-ci valident les transactions et les blocs, et transmettent l'information aux autres nœuds), ou être un client léger (ne téléchargeant que les entêtes des blocs, ce qui lui permet d'avoir une taille 1 000 fois inférieure à celle du nœud complet – mais le client léger doit se reposer sur les nœuds complets pour effectuer une transaction). Par ailleurs, les utilisateurs peuvent choisir d'être clients *Web* : l'accès au réseau bitcoin se fait alors à travers un navigateur connecté à un serveur-tiers de confiance.

Le manque de liquidité

Le bitcoin a été conçu pour être une monnaie dont la masse monétaire maximale a été fixée à 21 millions d'unités. L'émission de monnaie se fait par la récompense attribuée au premier mineur ayant miné un nouveau bloc [15]. Cette récompense, initialement de 50 bitcoins, est divisée par un facteur deux tous les 210 000 blocs minés, soit environ tous les quatre ans. À l'horizon 2140, la récompense sera inférieure à la plus petite unité, le « satoshi », qui vaut 10-8 bitcoins : il n'y aura alors plus aucune émission de monnaie et les mineurs seront rémunérés exclusivement par les frais des transactions.

---

(6) Cela se produit quand deux mineurs minent en même temps deux blocs différents. En fonction des délais de propagation dans le réseau (temps de latence), ces deux blocs peuvent arriver à certains mineurs dans un ordre donné, et à d'autres mineurs dans l'ordre inverse, ce qui a pour effet de scinder la blockchain *en deux chaînes. En pratique, les deux communautés de mineurs continuent à miner des blocs pour allonger les deux chaînes jusqu'au moment où l'une d'entre elles devient plus longue que l'autre : elle sera alors considérée comme la chaîne valide (et l'autre sera abandonnée).*

(7) Par exemple, deux blocs peuvent être minés l'un à la suite de l'autre dans la même chaîne, mais arriver dans l'ordre inverse dans un nœud de réseau (le deuxième bloc est alors appelé orphelin, il est mis temporairement dans un pool dans l'attente de l'arrivée du premier).

(8) En général, l'utilisateur paie des frais pour chaque transaction, ceux-ci vont au mineur ayant réussi à résoudre le bloc contenant la transaction. Plus les frais sont élevés, plus la transaction a des chances d'être intégrée en priorité au bloc miné suivant.

(9) CROMAN (Kyle) et al.*, "On Scaling Decentralized Blockchains", http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf*

(10) EYAL (Ittay) et al.*, "Bitcoin-NG: A Scalable Blockchain Protocol", https://arxiv.org/pdf/1510.02037.pdf*

(11) POON (Joseph) & DRYJA (Thaddeus), "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", https://lightning.network/lightning-network-paper.pdf

(12) HEILMAN (Ethan) et al.*, "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub", https://eprint.iacr.org/2016/575.pdf*

(13) DECKER (Christian) & WATTENHOFER (Roger) (2013), "Information Propagation in the Bitcoin Network", 13-th IEEE International conference on Peer-to-Peer Computing*, Trento, www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf*

(14) Aujourd'hui, pour un nœud complet, on conseille 125 Go d'espace sur le disque dur, 2 Go de mémoire RAM et une connexion Internet d'au moins 400 kb/s, https://bitcoin.org/en/full-node

(15) La récompense attribuée au mineur ayant miné le bloc a été prévue dès la conception du bitcoin afin d'encourager les opérations de minage.

Selon certains économistes, une diminution de l'émission monétaire pourrait créer un effet déflationniste. Les porteurs de bitcoins seraient alors tentés d'utiliser cette monnaie comme valeur de trésorerie, plutôt que comme instrument d'échange. À cela s'ajoutent les problèmes des bitcoins stockés dans des portefeuilles perdus (clé privée perdue) qui resteront dormants dans la *blockchain*. En conséquence, la valeur des bitcoins augmenterait, ce qui (à masse monétaire constante) diminuerait la liquidité des transactions (surtout dans un environnement déflationniste).

On oppose à ces critiques le fait que la division du bitcoin est très fine, la plus petite unité étant le « satoshi », soit 10^{-8} bitcoin. En cas de déflation, la monnaie pourrait se décaler (d'une ou de deux décimales) vers des valeurs plus faibles. De plus, il existe des *altcoins* d'une valeur inférieure (comme le Litecoin ou le Dogecoin) vers lesquels le bitcoin pourrait se rabattre pour compléter l'offre d'échange et empêcher ainsi la déflation, ou encore des *altcoins* comme Blackcoin, NXT, Peercoin ou VeriCoin, dont la masse monétaire est illimitée.

La déflation a mauvaise réputation, car elle est associée à l'effondrement brutal de la demande et peut conduire à une crise économique majeure. Actuellement, notre système financier dispose d'une monnaie fiduciaire dont l'émission est pratiquement illimitée et, en cas de déflation, une solution est d'augmenter la masse monétaire en imprimant des billets afin de relancer la demande. Dans le système du bitcoin, la déflation ne serait pas due à un effondrement brutal de la demande, mais à une réserve monétaire limitée et établie d'avance (toutefois, cette limite supérieure sera atteinte progressivement et ne causera pas automatiquement de crise financière).

La consommation d'électricité

Pour miner les blocs et ainsi valider les transactions, les mineurs doivent résoudre des problèmes cryptographiques difficiles, ce qui demande de grands volumes de calcul, et donc une consommation importante d'énergie (pour faire fonctionner les ordinateurs et les installations de refroidissement).

La difficulté du problème cryptographique à résoudre ne dépend pas du nombre et de la valeur des transactions, mais de l'arrivée de nouveaux mineurs attirés par les perspectives de gain financier et disposés à entrer sur ce marché concurrentiel. La rentabilité de leur activité dépend du prix de l'électricité converti en bitcoins.

Une étude a montré qu'en 2014, le réseau bitcoin consommait entre 0,1 et 10 GW [16]. Actuellement, l'ASIC (*Application-Specific Integrated Circuit*) le plus performant du marché (AntMiner S9) consomme 1 300 W, pour une vitesse de hachage de 13 THash/s, soit 100 W par THash/s. L'ensemble des mineurs du réseau bitcoin effectuent en moyenne 4 millions de THash/s, ils consomment donc 400 MW, ce qui représente la moitié de la puissance d'une centrale nucléaire. En pratique, comme les mineurs utilisent aussi des outils moins performants, cette consommation serait 3 à 4 fois plus importante que la valeur précédemment calculée [17].

Ce coût énergétique considérable doit être comparé aux économies potentielles que les institutions financières pourraient réaliser en remplaçant leur système de fonctionnement centralisé par le protocole *blockchain*. Selon Santander InnoVentures, en 2022, la technologie *blockchain* pourrait réduire les coûts d'infrastructure des banques de 15 à 20 milliards de dollars par an [18].

Une critique fondée formulée à l'encontre du protocole bitcoin est le fait que l'algorithme de preuve de travail ne sert qu'à assurer la sécurité du système et qu'il serait donc plus intéressant de l'associer à la résolution d'un problème utile, comme cela a été fait dans le cas des *altcoins* Primecoin (recherche de nombres premiers jumeaux et des chaînes de Cunningham), Curecoin (recherche de repliement de protéine) ou Gridcoin (grilles de calcul de recherche scientifique).

Les problèmes de sécurité

Le plus sérieux est l'attaque du type 51 % : un mineur ou un groupe de mineurs mal intentionnés disposant d'une grande capacité de calcul pourrait prendre le contrôle de la *blockchain* et utiliser celle-ci pour créer des « doubles dépenses ». Cela consiste à payer un produit, à entrer en sa possession, puis à créer intentionnellement une fourche, dont la nouvelle chaîne invalide la transaction et utilise l'argent pour acheter un deuxième produit (double dépense). Si sa puissance de calcul dépasse 51 % de la puissance totale des mineurs du réseau, un mineur mal intentionné aura la possibilité de miner des blocs dans la nouvelle chaîne de manière à dépasser l'ancienne, qui, de ce fait, sera invalidée.

Un mineur pourrait également effectuer une attaque de déni de service contre d'autres participants du réseau bitcoin en invalidant leurs transactions. Il suffit d'identifier la transaction correspondante, puis de re-miner le bloc qui la contient, en prenant soin de l'en enlever préalablement. La transaction restera en attente aussi longtemps que l'attaquant dominera le réseau des mineurs en puissance de calcul.

Selon certains modèles probabilistes, il ne serait même pas nécessaire de disposer de 51 % de la puissance totale de calcul du réseau : 30 % suffiraient. Cependant, vu la puissance totale de calcul du réseau bitcoin, il serait très difficile pour un mineur solitaire d'atteindre ce seuil de 30 % – ce qui serait en revanche possible pour un *pool* de mineurs. Ce dernier serait géré par un chef de *pool* qui construirait les blocs à miner, puis distribuerait ceux-ci entre les membres du *pool* pour effectuer l'opération de minage. Il aurait alors la possibilité d'exclure certaines

(16) J. O'DWYER (Karl) & MALONE (David), Bitcoin Mining and its Energy Footprint*, ISSC 2014 / CIICT 2014, https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf*
(17) http://digiconomist.net/bitcoin-energy-consumption
(18) The Fintech 2.0 Paper: rebooting financial services*, www.finextra.com/finextra-downloads/newsdocs/the fintech 2 0 paper.pdf*

transactions et d'inclure des doubles dépenses à l'insu des autres membres du *pool*.

Un moyen de défense contre ces attaques pourrait consister à modifier le protocole de la preuve de travail. Si le protocole nécessitait des capacités plus importantes en termes de puissance processeur ou de mémoire vive, cela rendrait plus chers les outils de calcul, alors qu'actuellement le prix des ASIC spécialisés est abordable.

Il peut y avoir par ailleurs des attaques malveillantes dont le but n'est pas de faire des profits financiers frauduleux, mais de perturber, voire de paralyser le réseau bitcoin en compromettant massivement les opérations de minage avec du déni de service. Une telle attaque nécessiterait de grands moyens (lesquels ne seraient probablement qu'à la portée d'un État).

Néanmoins, au fur et à mesure que la puissance totale de calcul du réseau bitcoin augmentera, les attaques seront de plus en plus difficiles à mettre en œuvre.

Défis juridiques, sociétaux et réglementaires

Le changement de comportement des utilisateurs

Dans le système bancaire classique, en cas d'erreur, d'oubli de mot de passe, de perte de chéquier ou de carte bleue, les porteurs ont un interlocuteur à qui s'adresser (l'établissement bancaire). L'utilisation des bitcoins demande à l'usager beaucoup plus de discipline : perdre une clé privée équivaut à perdre l'argent disponible sur les adresses engendrées à partir de cette clé privée, et il n'existe aucun moyen de le récupérer. Plusieurs porteurs ont connu de telles mésaventures à l'occasion d'un changement d'ordinateur ou de disque dur, car ils n'avaient pas pris soin de sauvegarder préalablement leurs clés privées [19].

L'utilisation des bitcoins demande donc un changement de comportement de la part des porteurs : il faut impérativement conserver les clés privées et les mots de passe, faire des copies sur plusieurs clés USB ou sur du papier, voire les graver sur du métal et les conserver dans plusieurs endroits sûrs.

La cybersécurité

Une clé privée peut également être volée, ce qui équivaut au vol de la somme totale d'argent disponible sur les adresses du portefeuille électronique générées avec ladite clé. Dans un monde où les cyberattaques sont de plus en plus fréquentes, il faut renforcer les mesures de cybersécurité habituelles : mettre à jour les logiciels et les antivirus, ne pas répondre aux messages électroniques douteux ou ne pas cliquer sur les fichiers attachés, éviter de naviguer sur des sites *Web* suspects, ne pas télécharger des fichiers provenant de sources non vérifiées.

Il est conseillé d'éviter les bourses de change ou les portefeuilles en ligne fournissant des services client *Web*, car ils n'offrent pas encore suffisamment de garanties de sécurité pour entreposer l'argent : il est préférable d'être « client complet » afin de disposer de l'ensemble de la *blockchain*. Il est aussi recommandé d'utiliser plusieurs portefeuilles, d'effectuer les transactions de faibles montants à partir d'un terminal mobile (client léger), moins sécurisé, d'effectuer celles de montants élevés à partir d'un ordinateur fixe (client complet). Le fait d'utiliser des transactions multi-signatures à partir de plusieurs clés privées réparties sur plusieurs supports différents (ordinateur de bureau, *smartphone*) augmente également la sécurité.

La vie privée

On entend souvent affirmer que le bitcoin est une monnaie anonyme, car on peut effectuer des transactions sans donner d'informations personnelles. Effectivement, les transactions contiennent les adresses des parties impliquées, qui sont générées à partir des clés publiques, lesquelles sont elles-mêmes générées à partir d'une clé privée. À partir d'une adresse, on peut connaître, *via* la *blockchain*, toutes les transactions dans lesquelles elle a été utilisée, mais on ne connaîtra pas l'identité de la personne. Cependant, si, par un malheureux concours de circonstances, l'identité de la personne liée à cette adresse était dévoilée, toutes les transactions qu'elle a effectuées en utilisant cette adresse seraient elles aussi dévoilées. Le bitcoin est donc une monnaie pseudo-anonyme.

C'est pourquoi il est conseillé d'utiliser plusieurs adresses, voire plusieurs portefeuilles, même si cela rend plus complexe la gestion personnelle des bitcoins.

La perception par le public

Le bitcoin a été l'objet dans le passé de plusieurs scandales, vols et escroqueries. Parmi les plus retentissants, on comptait (en février 2014) la faillite de la plateforme d'échanges de bitcoins MtGox, à la suite de la « disparition » de 774 000 bitcoins (409 M$) [20], ou (en août 2016) le vol de 120 000 bitcoins (72 M$) de la plateforme Bitfinex [21].

Le bitcoin reste perçu par une partie du public comme un réseau de blanchiment d'argent sale, ce qui affaiblit la confiance des utilisateurs.

Le changement sociétal

En général, les établissements financiers ont l'habitude d'« oublier » et de pardonner certaines erreurs aux clients, après un certain délai : ils donnent une deuxième chance aux clients ayant commis une faute dans un passé lointain. En revanche, un système fondé sur la *blockchain* « n'oublie jamais rien ».

L'absence de recours en justice

Dans le cadre des « contrats intelligents » (*blockchain* 2.0), les utilisateurs sont libres de décider des règles particulières à adopter, mais les transactions sont, quant à elles,

(19) Le Britannique James Howells a jeté à la poubelle le disque dur de son ordinateur avec un portefeuille électronique contenant 7 500 bitcoins : www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site
(20) www.theguardian.com/money/us-money-blog/2014/feb/25/bitcoin-mt-gox-scandal-reputation-crime
(21) http://fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/

irrévocables. Une fois choisies, ces règles doivent être respectées scrupuleusement, aucune déviation n'étant permise. Cela est renforcé par la technologie elle-même, indépendamment de la volonté des parties.

La réalisation d'un « contrat intelligent » est d'une grande efficacité et sans risque puisque l'on ne peut pas le contourner. Mais son extrême rigidité est le revers de la médaille : quelle place laisse-t-on à l'humain ? Comment procéder pour rompre un contrat intelligent ?

La taxation des transactions

Dans une économie décentralisée de partage pair-à-pair du type Uber ou Airbnb, ou faisant appel à des plateformes comme OpenBazaar pour effectuer des paiements en bitcoins, il est pratiquement impossible, pour l'État, de taxer les transactions. Par quels moyens l'État pourrait-il le faire ?

Conclusion

La *blockchain* pourrait devenir la couche économique et financière du *Web*. Elle permettra d'effectuer de façon décentralisée des paiements, des échanges, des transferts d'actifs, d'émettre et d'exécuter des contrats intelligents. Son domaine d'application peut aller au-delà des seuls aspects économiques et financiers.

Comme pour toute nouvelle technologie, l'implémentation de la *blockchain* peut connaître des obstacles et des limites. C'est à la communauté de ses acteurs qu'il revient de trouver les moyens permettant de les dépasser.

Bibliographie

ANTONOPOULOS Andreas, *Mastering Bitcoin*, O'Reilly Media, 2015.

CROMAN Kyle & *al*., *On Scaling Decentralized Blockchains,* http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

DECKER Christian & WATTENHOFER Roger, "Information Propagation in the Bitcoin Network", *13th IEEE International Conference on Peer-to-Peer Computing,* 2013, Trento University (Italy): www.tik.ee.ethz.ch/file/49318d3f56c-1d525aabf7fda78b23fc0/P2P2013_041.pdf

EYAl Ittay & *al*., *Bitcoin-NG: A Scalable Blockchain Protocol*, https://arxiv.org/pdf/1510.02037.pdf

HEILMAN Ethan & *al*., *TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub,* https://eprint.iacr.org/2016/575.pdf

NAKAMOTO Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*", https://bitcoin.org/bitcoin.pdf

J. O'DWYER Karl & MALONE David, *Bitcoin Mining and its Energy Footprint*, ISSC 2014 / CIICT 2014, https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf

POON Joseph & DRYJA Thaddeus, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, https://lightning.network/lightning-network-paper.pdf

The Fintech 2.0 Paper: rebooting financial services, www.finextra.com/finextra-downloads/newsdocs/the fintech 2 0 paper.pdf

Technologie des registres distribués : quel impact sur les infrastructures financières ?

Par Alexis COLLOMB
Titulaire de la chaire de Finance du Conservatoire national des Arts et Métiers (CNAM)
Klara SOK
Chercheuse et doctorante au CNAM
et Lucas LÉGER
Chercheur et doctorant au CNAM

On a beaucoup parlé de la technologie des registres distribués, et en particulier des *blockchains*, comme étant susceptibles de modifier en profondeur les infrastructures financières. En se focalisant sur les systèmes de paiement et les infrastructures de marché, cet article s'attachera tout d'abord à expliciter les raisons de l'engouement encore prudent des acteurs financiers pour cette technologie. Sont également évoqués les problèmes et les réticences à son adoption, notamment dus au nouveau paradigme de coopétition qu'elle présuppose. Par la suite, nous dresserons un état des lieux concis des dernières initiatives lancées par les institutions de paiement, les banques (en particulier les banques centrales) et les institutions internationales pour mieux saisir les possibilités de la technologie ou même, dans certains cas, la mettre déjà en production. Enfin, en conclusion, nous en évoquerons les perspectives d'avenir.

Introduction

Même si les expressions « technologie des registres distribués » (*distributed ledger technology* ou DLT) et « chaîne de blocs » (*blockchain*) sont utilisées de manière interchangeable par différents analystes, la seconde est *stricto sensu* un cas particulier de la première. Cette dernière procède de mises à jour régulières d'une base de données distribuée par constitution progressive d'une chaîne de blocs d'information liés par un chaînage cryptographique reflétant leur ordre chronologique.

Le développement récent de crypto-monnaies telles que le bitcoin et les différentes dérivations du protocole décrit dans le papier séminal de Satoshi Nakamoto ont suscité un intérêt très fort de la communauté financière. Si, d'un côté, la volonté affichée des *bitcoiners* de la première heure de se passer d'intermédiaires financiers en général, et des banques en particulier, ne pouvait laisser indifférentes les institutions financières, les diverses caractéristiques de la technologie (notamment sa traçabilité et son immutabilité) ne pouvaient que séduire une industrie dans laquelle les transactions foisonnent et pour laquelle le problème de la coûteuse gestion des données revêt un caractère crucial.

On a pu observer initialement une grande méfiance des institutions à l'encontre d'une technologie venue du bitcoin. Cette dernière a très souvent été associée à des ambitions de désintermédiation des tiers de confiance ou à des activités frauduleuses (en particulier dans le sillage de la faillite de la plateforme d'échange de bitcoins Mount Gox ou de la fermeture du site Silk Road). Cependant, il est vite apparu que la technologie dite de la « chaîne de blocs » avait probablement des atouts, que l'ensemble des acteurs de la communauté financière pourraient exploiter notamment pour réduire leurs coûts d'infrastructure. Ainsi, une étude de la Banque Santander et du Cabinet Oliver Wyman évoque une réduction des coûts des infrastructures financières de 15 à 20 milliards de dollars d'ici à 2022 [1].

Quelles sont les attentes des institutions financières ?

Plusieurs raisons sont évoquées par les institutions financières lorsqu'on les interroge sur leur intérêt pour cette technologie. Une étude récente de la Réserve fédérale

(1) Disponible à http://santanderinnoventures.com/fintech2/

américaine cite notamment les motivations suivantes [2] :

- réduire la complexité (en particulier dans les transactions transfrontalières multilatérales) ;
- améliorer la vitesse de traitement des transactions et la disponibilité des fonds et des actifs concernés (afin de réduire leur immobilisation et d'augmenter la liquidité) ;
- diminuer les besoins (souvent considérables) de réconciliation entre différentes infrastructures et différents registres ;
- augmenter la transparence et l'immutabilité des données transactionnelles en rendant celles-ci infalsifiables ;
- rendre les réseaux financiers plus résilients en introduisant une gestion distribuée des données ;
- réduire les risques opérationnels et financiers.

Si toutes ces aspirations à une organisation plus efficiente de l'infrastructure financière figurent clairement dans les recommandations publiées par la Banque des règlements internationaux [3], il faut avouer que cet attrait croissant de la technologie *blockchain* pour la sphère financière a été nourri par un contexte porteur avec, d'une part, la démonstration d'une certaine résilience et d'une certaine efficacité du réseau bitcoin pour les paiements internationaux et, d'autre part, quelques problèmes de sécurité posés par le réseau Swift. En effet, les utilisateurs du réseau bitcoin mettent en avant, parmi ses avantages, la rapidité des virements internationaux à moindre coût (si l'on fait abstraction des commissions de conversion de monnaie régalienne en bitcoin pour l'émetteur, et de conversion inverse pour le receveur). De plus, du fait de quelques fraudes d'envergure (comme celle d'environ 80 millions de dollars impliquant la Banque centrale du Bangladesh, début 2016), le réseau Swift n'a pas été épargné par une certaine publicité négative [4].

De toutes les raisons évoquées plus haut, les espoirs de désintermédiation et de réduction du travail de réconciliation entre les différentes contreparties sont probablement les plus importants – en particulier pour les transactions internationales, qui font souvent intervenir plusieurs intermédiaires [5]. Et ces espoirs de simplification se portent, au-delà des simples paiements internationaux, sur différents processus complexes souvent transfrontaliers, comme les activités de *trade finance*.

Ces perspectives de simplification des circuits financiers et de plus grande efficience sont encourageantes tant pour les acteurs financiers eux-mêmes que pour leurs usagers (entreprises ou particuliers). Ainsi, les banques régionales, qui aujourd'hui n'ont pas la possibilité de faire directement des virements internationaux, devraient pouvoir bénéficier d'un meilleur accès à une infrastructure de registre distribué. Quant à leurs homologues de plus grande taille, elles peuvent espérer des réductions de coûts significatives de leurs activités de *middle office* et de *back office*, comme nous l'avons déjà indiqué. Il ne faut pas oublier qu'aujourd'hui ces activités de réconciliation entre grands acteurs financiers sont encore en grande partie effectuées à la main, à l'aide de tableaux Excel. Bien sûr, les perspectives d'automatisation que le déploiement d'un registre distribué entre banques laisse entrevoir sont intéressantes pour ces institutions. Quant aux usagers (entreprises ou particuliers), ils sont en droit d'attendre d'un système simplifié des commissions moindres.

Mais à ces raisons classiques de réduction des coûts peuvent également venir se greffer des perspectives (sociétales ou de croissance) plus stimulantes. Ainsi, le Plan d'Action pour l'Inclusion financière du G20 de 2014 insiste sur la nécessité de réduire les coûts des paiements internationaux et d'utiliser les technologies innovantes pour permettre aux 2,5 milliards d'adultes exclus du système financier d'y être intégrés. L'accent est mis, également, sur le financement des PME (l'on estime à 2 000 milliards de dollars le « déficit de crédit » qui pourrait être comblé au profit de ces dernières [6]).

Enfin, l'intérêt pour la technologie des registres distribués vient également de perspectives attrayantes pour les régulateurs. En effet, il est tout à fait possible d'envisager le déploiement d'un tel système qui octroierait des droits d'accès sélectifs (principalement *read-only*) aux auditeurs ou aux régulateurs (pour lesquels l'accès serait confiné à certaines parties seulement du registre distribué).

Quels sont les freins au développement de cette technologie ?

Bien évidemment, les perspectives d'utilisation de la technologie des registres distribués ne sont pas sans poser un certain nombre de problèmes. Tout d'abord, certaines institutions financières auront du mal à envisager le remplacement de bases de données propriétaires par un registre distribué : étrange situation, en effet, que celle où il faut savoir coopérer avec ses compétiteurs (la coopétition) et partager ses données (même si l'on vous dit que l'on pourra définir précisément leur périmètre de confidentialité par du chiffrement). Ainsi, par exemple, pour que la mutualisation (*via* la mise en place d'un standard d'identité digitale) des procédures KYC (*Know Your Customers*) puisse bénéficier à tous, il sera nécessaire que chaque institution ait confiance dans l'intégrité du système : il faudra pour cela veiller à ce que les consultations de l'une ne puissent diffuser aux autres la liste de ses nouveaux clients.

Ensuite, l'utilisation de *blockchains* publiques (telles que celles du bitcoin ou d'Ethereum) n'est pas sans inquiéter des acteurs traditionnellement habitués à avoir le contrôle de leurs activités et de leurs infrastructures. Il n'est pas du

(2) https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf
(3) http://www.bis.org/cpmi/publ/d101a.pdf
(4) http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C
(5) La question de la valeur de l'intermédiation financière est une question déjà ancienne sur laquelle différents universitaires de renom se sont penchés. On pourra par exemple consulter l'article de Robert Merton sur ce sujet : A Functional Perspective of Financial Intermediation in Financial Management*, vol. 24, n°2, Silver Anniversary Commemoration (1995), pp. 23-41, disponible à l'adresse : http://www.people.hbs.edu/rmerton/afunctionalperspective.pdf*
(6) On pourra consulter ce plan d'action sur le site http://www.gpfi.org/

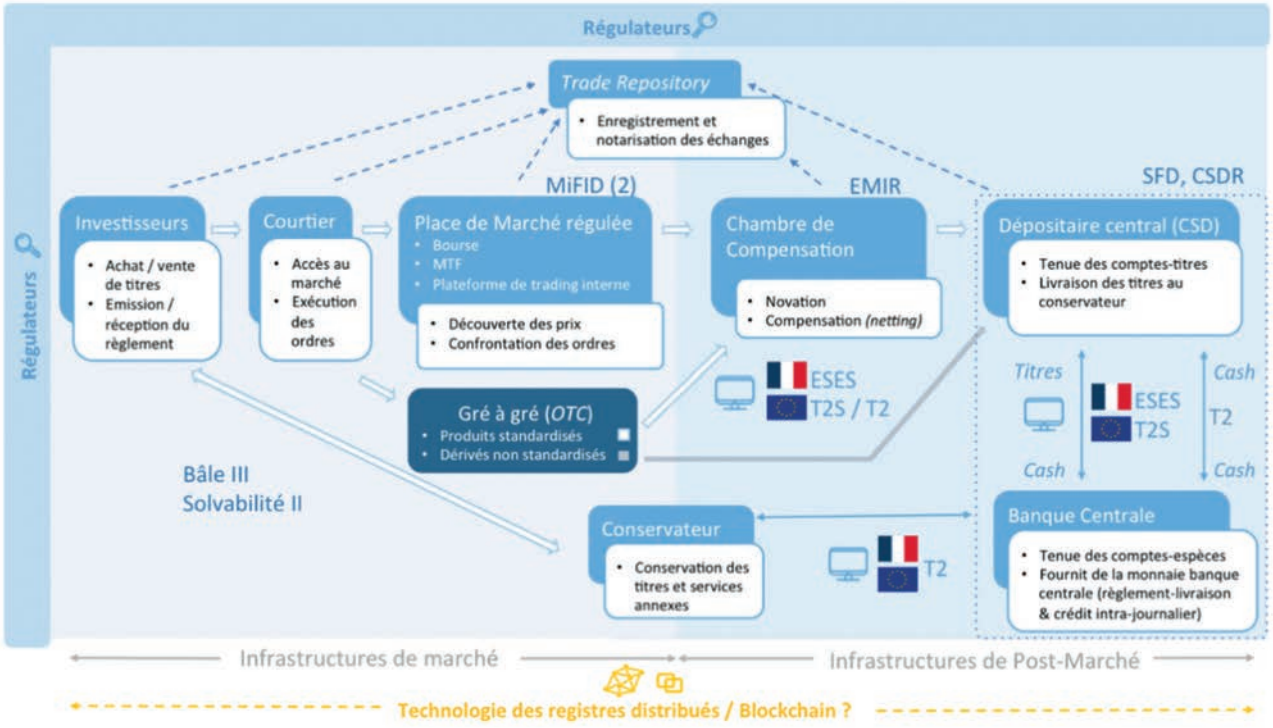


Figure 1 : Les possibilités d'implanter la *blockchain* pour réguler les circuits financiers « marché » et « post-marché ».

tout étonnant que les acteurs financiers s'orientent vers des systèmes permissionnés, et ce, dans une logique de consortium, tel R3 [7], qui regroupe aujourd'hui près de soixante-dix institutions.

Il y a également des problématiques d'intégration réglementaire. S'il est possible d'établir une correspondance assez étroite entre les réglementations en vigueur et l'architecture actuelle des marchés financiers (voir la Figure 1 [8] ci-dessus), il est intéressant de noter que l'Autorité européenne des valeurs mobilières (AEVM/SMA) estime cependant qu'il n'y a pas dans le cadre réglementaire européen d'obstacle majeur qui puisse empêcher l'émergence de la *Distributed Ledger Technology* (DLT) à court terme [9]. Cependant, il est certains cas où la réglementation en place pourrait être problématique pour la mise en place d'un registre distribué [10].

Mais il y a aussi d'autres problèmes, comme ceux de la gouvernance et de la répartition des responsabilités, dans le cas d'une infrastructure partagée. Si ce problème s'est déjà manifesté pour des *blockchains* publiques (voir l'expérience malheureuse de The DAO), il peut également se poser dans le cas d'un consortium, en particulier dans l'élaboration de ses standards. De plus, la mise en place de registres distribués devra être accompagnée d'ajustements des procédures d'évaluation et de consolidation des risques (qu'ils soient de crédit, de liquidité ou opérationnels).

Enfin, ces registres distribués devront être source d'autorité et de finalité juridique, ce qui est encore très loin d'être évident. En France, on aura par exemple vu échouer, l'année dernière, une proposition législative concernant « le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres dont le fonctionnement utilise la technologie dite de la *blockchain* », qui visait justement à faire considérer ces opérations comme des actes électroniques authentiques « de la même manière que [le sont] les actes passés devant notaire » [11].

De nombreuses initiatives en cours

Les initiatives liées à l'étude ou au déploiement de la technologie sont très nombreuses, mais elles en restent encore souvent au niveau de la preuve de concept. Pour les paiements, les grandes compagnies de cartes de crédit telles que Visa (avec B2B Connect) ou MasterCard (avec Mastercard Blockchain) ou des grands du *Web* tels que PayPal (avec sa filiale Paypal Braintree qui permet à des commerçants d'accepter des bitcoins comme moyen de paiement) commencent à être actifs. De même, des entreprises spécialisées dans les transferts d'argent internationaux (telles que Western Union) ont investi dans la technologie. Même Swift (membre de la fondation Hyperledger) a développé au début de cette année une preuve de

(7) http://www.r3cev.com/
*(8) On pourra également consulter par exemple le n°15 d'*Opinions & Débats *publié en mai 2016 par COLLOMB et SOK et disponible sur http://www.louisbachelier.org/*
(9) Voir le rapport ESMA50-1121423017-285 du 7 février 2017, disponible sur https://www.esma.europa.eu
(10) Voir : http://www.coindesk.com/distributed-ledger-cftc-post-trade-dodd-frank/, où les auteurs envisagent une difficulté liée à la législation Dodd-Frank pour gérer des swaps *sur un registre distribué.*
(11) http://www.assemblee-nationale.fr/14/amendements/3785/AN/227.asp

concept *blockchain* dans le cadre de son initiative globale sur les paiements. Enfin, il y a des passerelles, de plus en plus nombreuses, entre crypto-monnaies et monnaies régaliennes. Ainsi, la *start-up* Glidera, qui offrait à ses utilisateurs la possiblité d'acheter des bitcoins à partir de leur compte bancaire, a été rachetée par la plateforme Kraken, qui propose également d'utiliser Swift pour des dépôts en dollars américains ou en livres anglaises ou d'effectuer des virements SEPA en euros [12]. Il faut également noter la mise en production de l'initiative de Ripple, qui permet désormais d'effectuer des paiements interbancaires et internationaux dans les institutions bancaires de neuf pays [13].

Pour les marchés financiers, il y a eu de très nombreuses initiatives, mais celles-ci restent en général limitées à des sous-jacents non cotés (par exemple, l'initiative Linq du Nasdaq) ou de niche. L'initiative la plus avancée semble être celle de l'échange de *securities* australien ASX, qui travaille avec Digital Asset Holdings et qui envisage de remplacer son système de compensation CHESS par un registre distribué. Il existe de nombreuses autres initiatives, telles que celles de SETL, Clearmatics ou Euroclear, mais celles-ci semblent être moins abouties.

Quant aux banques centrales, elles ne sont pas en reste : elles ont presque toutes lancé des initiatives liées à l'étude de la technologie : la Banque de France a ouvert en début d'année un laboratoire dédié à la *blockchain* [14] ; la Banque d'Angleterre est en partenariat avec Ripple pour le développement d'un système de paiement international multidevises entendant montrer comment la synchronisation permise par la technologie devrait « permettre de réduire le risque de règlement et améliorer la vitesse et l'efficience des paiements transfrontaliers [15] » ; la Banque populaire de Chine s'est penchée sur le cas du bitcoin depuis 2014 et est en train d'expérimenter la mise en place de sa propre crypto-monnaie, en liant celle-ci à une plateforme d'échange de papier commercial basée à Shanghai (ce développement semble s'effectuer parallèlement à une supervision renforcée des échanges bitcoin depuis le début de l'année).

Cette réflexion sur l'utilisation de la technologie pour la mise en place de « crypto-monnaies régaliennes » a également été l'un des thèmes centraux de la 16ème conférence internationale sur les défis du secteur financier organisée par la Réserve fédérale américaine à Washington, avec le FMI et la Banque mondiale.

Conclusion

Il paraît naïf de penser que le développement de la technologie des registres distribués risque de faire disparaître les intermédiaires financiers. Si l'on regarde le cas de la première des *blockchains*, celle du bitcoin, on constate que l'écosystème a favorisé l'éclosion de nouveaux intermédiaires (à commencer par de nouveaux échanges).

Si l'on peut envisager différents scénarios d'intégration de la technologie au sein de l'infrastructure postmarché (qu'il s'agisse de compensation, de règlements ou de conservation), il n'y a pas encore de consensus d'experts sur la question et l'acceptabilité de la *blockchain* risque de s'installer graduellement [16] en parallèle à l'automatisation progressive des processus (l'on peut néanmoins s'attendre à ce que la technologie ait un impact plus rapide sur les systèmes de paiement).

L'interopérabilité des différents registres sera un problème clé, et qu'il s'agisse de *blockchains* publiques ou de *blockchains* privées, la capacité des différents écosystèmes à interagir entre eux et à établir des normes et des standards risque d'être un élément essentiel de leur développement, et une condition nécessaire de leur succès [17]. Mais si l'on doit encore rester prudent, surtout à court terme, sur les chances de déploiement à grande échelle des registres distribués, la technologie – qui semble aujourd'hui être sortie de sa phase de *hype* pour commencer sa phase de maturation [18] – aura en tout cas remis les projecteurs sur l'impact croissant de la transformation numérique. Et une chose est sûre : cette dernière n'est pas près de s'arrêter !

(12) https://www.kraken.com/
(13) https://ripple.com/
(14) Discours de François Villeroy de Galhau, Gouverneur de la Banque de France et président de l'Autorité de Contrôle prudentiel et de Résolution, au Paris FinTech Forum du 25 janvier 2017.
(15) Dernière annonce faite sur le site de Ripple, le 17 mai 2017.
(16) On pourra consulter https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf
(17) On pourra, par exemple, consulter le projet https://interledger.org/interledger.pdf
(18) On se réfère ici à la typologie de Gartner (www.gartner.com) pour les technologies émergentes.

Les enjeux de la *Blockchain* pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR)

Par Nathalie BEAUDEMOULIN
Coordinatrice du Pôle FinTech Innovation de l'Autorité de Contrôle prudentiel et de Résolution
Didier WARZÉE
Ingénieur des mines, expert au Pôle FinTech Innovation de l'Autorité de Contrôle prudentiel et de Résolution
et Thierry BEDOIN
Chief Digital Officer de la Banque de France

L'Autorité de Contrôle prudentiel et de Résolution (qui contrôle les banques et les assurances) ainsi que la Banque de France se sont structurées pour répondre aux défis de la révolution technologique à l'œuvre dans les services financiers. La *blockchain* fait partie des sujets technologiques susceptibles d'optimiser, voire de modifier la manière dont les activités financières peuvent être traitées et fournies. Toutefois, cette technologie reste peu mature et devra dépasser quatre grands dilemmes avant de pouvoir être utilisée pour réaliser des opérations financières.

Une *blockchain* ou des *blockchains* ?

Le terme de *blockchain* (ou d'autres termes proches) est parfois utilisé improprement pour désigner des dispositifs informatiques pouvant être en réalité très différents les uns des autres tant dans leur conception qu'au regard des principes qui les sous-tendent. Au-delà des dénominations, le régulateur s'attachera tout d'abord à examiner les caractéristiques essentielles des solutions présentées pour fonder sa position.

Ainsi, historiquement, le terme « *timestamp server* » a été utilisé pour désigner le protocole sous-tendant le bitcoin, avant que n'apparaisse (peu de temps après) le terme de *blockchain*. Du fait du rôle pionnier de la combinaison de diverses solutions technologiques ayant permis de créer le bitcoin, ce terme est maintenant régulièrement utilisé pour des modèles présentant des similarités avec celui-ci, mais aussi, souvent, pour des modèles présentant avec le bitcoin des différences significatives. Dans certains cas, l'acronyme DLT (pour *Distributed Ledger Technology*) est aussi mis en avant de manière à se démarquer (notamment pour des raisons d'image) de la crypto-monnaie bitcoin.

En effet, le bitcoin, qui n'est pas considéré comme une monnaie ayant cours légal, présente des risques intrinsèques forts tant pour les consommateurs – forte volatilité, risque de fraude avéré – qu'au regard des exigences de lutte contre le blanchiment des capitaux et le financement du terrorisme, notamment du fait de l'anonymat des détenteurs qui se heurte au principe fondamental d'identification du client dans le domaine financier. Le bitcoin a donc légitimement fait l'objet de prises de positions vigoureuses des autorités, tant françaises qu'européennes [1], visant à révéler ces risques au public et à les prévenir autant que possible. Dès lors, les promoteurs de solutions technologiques du type *blockchain* cherchent parfois à se prémunir contre l'assimilation de celles-ci au bitcoin.

Pour autant, certains d'entre eux vont en réalité promouvoir une solution entièrement décentralisée, qu'ils présentent, du fait de la disparition espérée d'intermédiaires, voire de l'autorité centrale d'administration, comme un vecteur majeur de transformation des services financiers, voire même de la Société.

(1) Position 2014-P-01 du 29 janvier 2014 de l'ACPR relative aux opérations sur bitcoins en France. Le fonctionnement du bitcoin, ses risques pour les utilisateurs et les enjeux d'un encadrement réglementaire sont aussi détaillés dans le Focus *n°10 du 5 décembre 2013 publié sur le site Internet de la Banque de France, ainsi que dans le communiqué d'alerte émis le 12 décembre 2013 par l'Autorité bancaire européenne (www.eba.europa.eu).*

La technologie se met alors au service d'une philosophie que l'on peut qualifier de libertaire, qui promet le retour (primitif, bien que numérique) à des relations financières directes entre individus s'appuyant sur un mécanisme transactionnel de confiance entièrement décentralisé.

Mais au-delà de ces cas assez utopiques, la technologie *blockchain* présente des caractéristiques suffisamment remarquables pour que les acteurs financiers (qu'ils soient récents ou davantage établis) et les autorités financières (dont la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution) s'y intéressent de très près.

Quel est le potentiel de la *blockchain* publique décentralisée pour le domaine financier ?

Au-delà du bitcoin en tant que monnaie virtuelle, c'est l'ensemble du mécanisme de confiance mis en œuvre par celui-ci qui a soulevé l'enthousiasme et aiguisé la créativité d'acteurs financiers, notamment de nombreuses *start-ups* qui y voient une façon de concurrencer les établissements financiers.

En effet, le – ou les – créateurs du bitcoin ont pensé sa *blockchain* originelle comme un système décentralisé ne faisant appel à aucun tiers de confiance et se fondant sur des techniques cryptographiques pour assurer simultanément la transparence, la sécurité et l'anonymat de transactions numériques directes de pair-à-pair. Ainsi, un registre entièrement transparent de transactions directes de pair-à-pair distribué sur un nombre important de nœuds d'un réseau est, de ce fait, présenté comme indestructible. De plus, son intégrité est garantie par un mécanisme impliquant, à chaque validation d'un nouveau bloc de transactions (sécurisée par le protocole de consensus par « preuve de travail »), l'intégration de l'empreinte numérique de la chaîne de blocs précédente.

Une qualité que souhaitent fréquemment utiliser des porteurs de projet est l'inaltérabilité de la base de données distribuée, avec la confiance qu'elle est censée générer afin de sous-tendre des projets de registres d'informations ou de transactions – *via* l'utilisation de *tokens* – dans le monde réel.

Toutefois, au-delà de ces atouts, des limitations significatives sont rapidement apparues ne serait-ce qu'en matière de volumes de transactions traitables ou de délais nécessaires à ce traitement, qui ont donné naissance à d'autres dispositifs visant à compenser ces lacunes. C'est ainsi que d'autres *blockchains* publiques ont vu le jour, telle la *blockchain* Ethereum, qui intègre des contrats s'exécutant de manière automatisée (les *smart contracts*) dès lors qu'une information externe (appelée oracle) en déclenche la réalisation, le projet de *blockchain* Hyperledger dédiée au *business*, ou encore la *blockchain* Tangle/IOTA spécialisée dans les problématiques d'objets connectés.

Les *smart contracts* permettraient, en interagissant « intelligemment » avec le monde réel, d'envisager des actions plus sophistiquées qu'une simple transaction réalisée en crypto-monnaie (y compris améliorée par la possibilité d'y associer quelques octets de caractères, dans le cas du bitcoin). Ainsi, par exemple, certains modèles assurantiels sont fondés sur ce type de mécanisme, proposant une indemnisation automatique sur le fondement d'un *smart contract* se référant au tableau des arrivées des avions d'un aéroport (assurance retard).

Toutefois, 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.
- 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 point [2]). L'emprise de ces parties prenantes sur le fonctionnement des *blockchains* publiques défie le caractère « démocratique » affiché et elle peut provoquer de vrais schismes dans les communautés, qui se traduisent parfois par des scissions de la *blockchain* elle-même (*hard fork*). Elle pose *in fine* la question de leur gouvernance, car les tiers de confiance auxquels ces *blockchains* sont censées se substituer ne font, dans ces conditions, que se « déplacer » et revenir sous d'autres formes (développeurs, mineurs), d'une manière beaucoup moins transparente, et en ayant des objectifs souvent divergents.
- 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

(2) 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).

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.

Conséquence : on envisage de réintégrer une autorité centrale dans des protocoles de registres distribués

Les acteurs financiers ont donc cherché à recréer des systèmes inspirés des *blockchains* publiques, à ceci près qu'ils en resteraient l'autorité centralisatrice tiers de confiance, permettant ainsi de résoudre certains des problèmes susmentionnés – tout en conservant dans le système ainsi créé une position privilégiée s'inscrivant dans la continuité de leurs fonctions actuelles.

Le cas le plus orthogonal aux *blockchains* publiques est celui de registres distribués entièrement privés. Dans la pratique, ils correspondent plutôt à des bases de données de transactions répliquées sur plusieurs sites physiques et bénéficiant des mécanismes cryptographiques assurant leur intégrité, sans toutefois se fonder sur des mécanismes de minage. Ceux-ci sont en effet rendus superflus par une confiance *a priori* forte entre des nœuds exhaustivement contrôlés par le même acteur.

Ces *blockchains* privées sont notamment utilisables pour optimiser des procédures internes, au sein de groupes. Elles peuvent ainsi permettre de disposer d'un outil d'enregistrement immédiat et partagé d'informations et de transactions entre différentes sociétés d'un même groupe, ou entre différentes unités d'une même entreprise. Le rôle du superviseur consistera alors à surveiller les risques opérationnels (dont les problèmes de cybersécurité, les risques liés à l'utilisation éventuelle du *cloud*, etc.) que ces solutions font éventuellement courir aux établissements financiers, et ce de la même manière que pour toute autre utilisation de nouvelles technologies de gestion de l'information, sans que cela ne soit uniquement et spécifiquement lié au recours à la *blockchain*.

Les limitations en matière de cas d'usage de ces *blockchains* privées (notamment pour ce qui concernerait des activités BtoC) ont conduit au développement de modèles impliquant une architecture proche de celle des *blockchains* publiques, mais avec des mécanismes conférant à un tiers central la gestion de la gouvernance, du code et des accès au dispositif : elles sont fréquemment appelées « *blockchains* publiques permissionnées ».

L'expression de « *blockchain* publique permissionnée » est toutefois susceptible de recouvrir des systèmes assez différents ; de celui qui n'autorisera que quelques acteurs dans le réseau pair-à-pair en organisant une gouvernance spécifique du code utilisé – système en général dit des *blockchains* de consortium quand ces acteurs sont des sociétés –, à un système d'accès en théorie ouvert utilisant un protocole de consensus calqué sur le mécanisme public, mais intégrant un acteur centralisant les droits d'accès et certaines informations concernant les utilisateurs.

Au regard des cas d'usage, et notamment de la « confiance *a priori* » entre les pairs du réseau, le protocole de consensus sera souvent différent de la « preuve de travail » du bitcoin, ce qui améliorera substantiellement la rentabilité du système (le coût énergétique du « minage » du bitcoin étant en effet très important).

Il y a aussi des projets de systèmes permissionnés qui cherchent à retrouver des propriétés de résilience du registre (intégrité et disponibilité) proches de celles des *blockchains* publiques. Or, ces propriétés sont générées par la taille des réseaux (plus celle-ci est importante et plus il existe de copies du registre) et par l'énergie dépensée par les mineurs pour la validation des blocs, dans le cas du consensus « preuve de travail » : plus celle-ci est importante, plus un éventuel attaquant devra lui-même dépenser d'énergie pour corrompre le système. Une solution envisagée, dite *sidechain*, consiste à ce qu'une *blockchain* publique permissionnée se branche (en quelque sorte) sur une *blockchain* publique non permissionnée afin de pouvoir être sécurisée.

La plupart des cas d'usage envisagés aujourd'hui, que ce soit dans le cadre des ouvertures réglementaires françaises (enregistrement et transactions sur les titres non cotés [3]) ou dans celui d'autres projets liés à la gestion d'actifs, aux paiements, aux transferts de fonds ou à l'assurance, le sont au travers d'un modèle *blockchain* publique permissionnée.

Au vu des différences significatives dans ce que ces modèles recouvrent en réalité, il faudra examiner au cas par cas les projets proposés afin de déterminer de quelle façon ils répondent aux exigences réglementaires.

De manière générale, les dispositifs proposés doivent d'ores et déjà se conformer aux exigences fondamentales que sont la sécurité des transactions, la protection du consommateur et la lutte contre le blanchiment des capitaux et contre le financement du terrorisme. Ainsi, les clients devront toujours être identifiés de manière fiable et documentée (au moyen de mesures d'identification renforcées si l'entrée en relation ne s'effectue pas en face-à-face). Les paiements qui transiteraient par un tel dispositif devront toujours être entourés des mesures de sécurité requises (par exemple, l'authentification renforcée). Les dispositifs doivent aussi respecter les exigences

(3) L'article 120 de la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique habilite le gouvernement, d'ici le 9 décembre 2017, à réformer le droit applicable aux titres financiers afin de permettre la représentation et la transmission (au moyen d'un dispositif d'enregistrement électronique partagé) des titres financiers qui ne sont ni admis aux opérations d'un dépositaire central ni livrés dans un système de règlement et de livraison de certains instruments financiers.

Photo © Romain Gaillard/REA

La *Fintech Revolution*, événement organisé par France Fintech, le 28 mars 2017 (seconde édition), au théâtre de La Gaîté Lyrique.

« L'Autorité de Contrôle prudentiel et de Résolution s'est dotée en juin 2016 d'un pôle dédié aux *FinTechs* et à l'innovation. »

réglementaires spécifiques applicables aux cas d'usage (comme, les informations précontractuelles, dans le cadre de souscriptions de contrats).

Les établissements doivent en outre tenir compte des réglementations trans-sectorielles susceptibles de s'appliquer, telles les nouvelles règles européennes liées à la protection des données personnelles [4] (dont le recueil du consentement du client avant tout traitement, le droit à l'oubli – qui apparaîtrait difficile à respecter si la *blockchain* restait immuable – ou encore les dispositions européennes liées à l'utilisation de la signature électronique [5]).

Une question attentivement suivie par le Pôle FinTech Innovation de l'ACPR et par la Banque de France

Afin d'être en phase avec la révolution numérique actuellement à l'œuvre dans les services financiers (dont la *blockchain* est l'une des manifestations) et de préparer la supervision d'une finance toujours plus digitale, l'Autorité de Contrôle prudentiel et de Résolution s'est dotée en juin 2016 d'un pôle dédié aux FinTech et à l'innovation.

Ce pôle travaille étroitement avec l'Autorité des Marchés Financiers, avec laquelle l'ACPR anime un Forum FinTech, qui réunit des FinTech, des banques et des assurances, ainsi que d'autres partenaires de l'écosystème de l'innovation financière, et les pouvoirs publics. Les sujets abordés portent sur la régulation de l'innovation et sur les problématiques réglementaires liées à la *blockchain*, telle que (par exemple) la valeur juridique des opérations enregistrées sous une *blockchain* ou encore les *smart contracts*.

En tant qu'autorité indépendante adossée à la Banque de France, l'ACPR entretient un dialogue constant avec les experts de la Banque centrale sur les enjeux liés à la *blockchain*. En effet, ayant rapidement perçu les enjeux de cette nouvelle technologie pour certaines de ses missions (systèmes de paiement et infrastructure de marchés, politique monétaire, services bancaires), la Banque de France a décidé de tester la *blockchain* afin d'être en mesure de juger par elle-même des potentialités de cette technologie.

Ainsi, la Banque de France conduit actuellement, sous l'égide de son *Chief Digital Officer,* plusieurs expérimen-

(4) Règlement (UE) 2016/679 du 27 avril 2016 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
(5) Règlement (UE) 910/2014 du 23 juillet 2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».

tations de la technologie *blockchain*, dont l'une, menée avec des banques de la place, vise à maintenir de manière décentralisée un registre d'identifiants ICS (identifiant créancier SEPA remplaçant le TIP depuis le 1er août 2014) utilisés dans les prélèvements SEPA (projet MADRE). Si les banques françaises s'échangent actuellement l'identité de leurs clients créanciers (ICS) grâce à l'intervention opérationnelle de la Banque de France qui centralise les demandes, génère et dissémine l'ensemble de ces identifiants, l'utilisation de la *blockchain* permet la tenue de ce registre dans les *smart contracts* d'une *blockchain* à laquelle les banques participent directement. La Banque de France réussit ainsi à exercer son rôle d'opérateur du service ICS au travers de traitements automatiques qui s'exécutent selon des règles prédéfinies qu'elle a déployées dans la *blockchain*. Dans la gouvernance du dispositif, elle conserve uniquement un rôle d'accréditation initiale des banques participantes, tout en renforçant sa qualité de tiers de confiance.

Cette expérimentation a confirmé une capacité de la technologie *blockchain* à relever des défis réels, notamment en matière de tenue de registre. Son extension à une *blockchain* interbancaire multiservices et son utilisation éventuelle dans des traitements critiques du monde de la finance dépendront néanmoins d'avancées restant à démontrer sur les aspects liés à la capacité de traitement de masse (*scalabilité*), à la confidentialité des transactions, à la sécurisation et, surtout, à la mise en place de dispositifs de gouvernance assurant son bon fonctionnement dans la durée.

Conclusion

Si certaines caractéristiques de la technologie sous-jacente à la *blockchain* peuvent être prometteuses, son application à des activités impliquant le traitement de flux financiers importants exigera que l'on ait au préalable relevé des défis notables dans les domaines technique et réglementaire.

La *blockchain*, un levier de digitalisation pour les banques de financement et d'investissement (BFI)

Par Éric ROSSIGNOL
Chargé de l'analyse quantitative et du laboratoire d'innovation pour le département Titrisation du Crédit Agricole CIB
et Xavier LAURENT
Membre de l'équipe Innovation et du département *Strategy & Business Transformation* et leader de la Communauté *Blockchain* du Crédit Agricole CIB

Si les banques de financement et d'investissement (BFI) (ou banques de gros) réalisent de nombreux prototypes sur la base de la *blockchain*, c'est parce que leurs activités sont largement basées sur la confiance qu'elles apportent à leurs clients. La confiance est en effet également le moteur de la *blockchain*. À ce jour, les BFI pensent que la *blockchain* est plus une opportunité de limiter les coûts et de rendre un meilleur service à leurs clients qu'une menace. En effet, les entreprises continuent à avoir besoin d'un fournisseur de liquidités au meilleur prix.

Introduction

Le temps où l'innovation était l'apanage du cadre professionnel, où la majorité des collaborateurs avaient accès à un matériel de pointe à leur travail et pouvaient parfois en faire bénéficier leur foyer, est aujourd'hui révolu.

Le digital s'est d'abord développé auprès du grand public, celui-ci étant plus ouvert que les entreprises à l'expérimentation de nouveaux usages, avec les risques que ceux-ci comportent. En revanche, le rythme de la digitalisation de l'environnement professionnel a ralenti. Cela s'est traduit par un sentiment de frustration parmi les salariés des entreprises.

Par ailleurs, les grands groupes (notamment industriels) reposent sur des strates de systèmes d'information construites sur de longues périodes (parfois depuis les années 1960) qui freinent leur démarche d'innovation et qui donnent un avantage certain aux petites et moyennes entreprises, plus agiles qu'eux et dont les systèmes d'information sont plus récents. Cet avantage est particulièrement important pour les *FinTechs* (les *start-ups* de l'industrie financière utilisant les nouvelles technologies) par rapport aux banques traditionnelles.

Face à ces évolutions, les banques de financement et d'investissement doivent répondre aux attentes nouvelles de leurs clients et accompagner leurs expériences digitales par une efficacité d'exécution accrue. Cela ne pourra être fait sans une adoption des nouvelles technologies allant de pair avec une révision en profondeur de leurs processus. En revanche, elles ne doivent pas oublier qu'elles seront les garantes de la sécurisation des solutions qu'elles apporteront, la maîtrise des risques restant pour leurs clients un élément différenciant vis-à-vis de la concurrence nouvelle des *FinTechs*.

La *blockchain* et ses dérivées, les technologies de registres distribués (DLT), sont des éléments de réponse importants, car ils pourraient apporter la confiance nécessaire aux institutions financières, à leurs clients, aux régulateurs ainsi qu'à de multiples acteurs des domaines de l'échange d'informations et de l'automatisation digitale dans un environnement sécurisé.

La disparition inéluctable du tiers de confiance ?

À l'origine du bitcoin, il y avait le souhait de s'affranchir du système financier traditionnel (des banques et des banques centrales) et de proposer une alternative purement technologique à leur rôle de tiers de confiance validant le transfert de valeur. Après un peu moins de dix ans de recul sur ce phénomène, force est de constater que les banques, bien qu'elles soient en pleine transformation digitale, jouent toujours ce rôle. Pour l'utilisateur non informaticien chevronné, l'usage de bitcoins lui permet certes de se passer d'une banque, mais cela le contraint à accorder sa confiance à un service tiers de conservation de son *wallet* (équivalent à un porte-monnaie électronique dans lequel sont déposés ses bitcoins) ou à échanger sa crypto-monnaie contre une monnaie traditionnelle plus large-

ment acceptée. Ce sont la plupart du temps ces nouveaux tiers de confiance qui se font prendre en défaut par les pirates et qui sont responsables des vols de crypto-monnaie qui font les gros titres de la presse.

De manière analogue, le juriste détient une expertise qui lui permet de certifier la conformité juridique d'un contrat légal. Demain, le recours à un informaticien sera probablement nécessaire pour pouvoir valider la conformité pleine et entière du code définissant les *smart contracts*. Ainsi, il sera nécessaire de faire confiance à la personne en charge de coder le *smart contract*.

À titre d'exemple, les promesses d'Arcade City et La'Zooz[1], en tant que concurrents potentiels d'Uber, viennent confirmer une fois de plus qu'un tiers de confiance demeure nécessaire. Ces plateformes sont une nouvelle forme d'opérateur offrant plus de flexibilité et de liberté à leurs utilisateurs (notamment sur les prix). En revanche, elles restent les opérateurs donnant accès à la plateforme et à la technologie, et les utilisateurs acceptent de placer leur confiance dans la technologie qu'elles mettent à leur disposition et grâce à laquelle elles opèrent.

Contrairement à une idée reçue largement partagée, les BFI estiment généralement que la *blockchain* ne fait pas disparaître les tiers de confiance, mais qu'elle les redistribue sur la chaîne de valeur en transférant cette valeur vers la technologie et vers ceux qui la maîtrisent.

La promesse d'une vérité partagée

Les technologies numériques (portées, par exemple, par l'essor d'Internet) facilitent, depuis de nombreuses années, la digitalisation et l'accélération des échanges. Cela a été en particulier remarquable dans le cas des activités de marchés de capitaux avec leur informatisation progressive durant les années 1980-1990, la connectivité d'Internet et, finalement, le *trading* haute fréquence, depuis les années 2000. Ces différentes révolutions technologiques ont favorisé la croissance des marchés d'échanges et leur liquidité.

Une chose, cependant, n'a pas changé : chaque participant inscrit de son côté sa propre vision des échanges. La réconcilier avec celle de ses différentes contreparties demande un effort important et, même si, la plupart du temps, ces visions sont partagées, fréquemment des écarts subsistent. Ces écarts représentent un risque, mais, surtout, ils exigent une énergie considérable (et le coût y afférant) de la part des BFI afin de les expliquer. Malgré la présence de tiers de confiance (comme les chambres de compensation), pour une part importante de ces échanges, ces risques demeurent. Ils nuisent à l'efficacité des échanges, puisque le règlement s'effectue (en général, sur le marché Euro) deux jours plus tard, et ils ont un coût, puisque, sur cette période, le risque doit être provisionné.

Pour le régulateur, cette situation est également loin d'être idéale. Ayant besoin d'une visibilité toujours plus importante et exhaustive afin de mener pleinement son action de contrôle, il reçoit de la part de chaque acteur cette vision partielle qu'il se doit de réconcilier avec celle des autres acteurs et avec la sienne propre.

Les technologies de registre distribué ont la faculté de changer ce paradigme. Elles permettraient d'instaurer une vision unique et, par là même, une vision de référence, partagée entre l'ensemble des acteurs et des opérateurs d'un marché. Dans ce modèle, chacun aurait une vision limitée aux échanges sur lesquels il est intervenu, mais, d'une part, les écarts entre les différents acteurs devraient être nuls et, d'autre part, une vision globale et exhaustive serait offerte aux autorités de tutelle, qui pourraient alors jouer pleinement et de matière efficace leur rôle de contrôleur. Le règlement des échanges pourrait être effectué en fin de journée (voire plus fréquemment).

L'émergence de nouvelles plateformes digitales

Le *Trade Finance*[2] est une activité qui, jusqu'ici, a globalement résisté aux tentatives de digitalisation. Les principes de base posés par les banques génoises et vénitiennes au Moyen Âge perdurent aujourd'hui, même s'ils se sont complexifiés et sophistiqués avec le temps. Le document papier règne encore en maître, passant de main en main, de signature en tampon, jusqu'à l'expertise nécessaire à sa reconnaissance. Le coût et le temps nécessaires à la gestion des documents papier sont très significatifs.

C'est là le prix à payer pour qu'un grand nombre d'acteurs privés et publics d'horizons différents puissent instaurer entre eux la confiance minimale requise pour que l'échange de valeurs contre des produits ou services puisse avoir lieu par-delà les frontières et les territorialités.

Aux yeux du banquier, son rôle est toujours d'accompagner les importateurs et les exportateurs dans leurs échanges en leur permettant de financer leurs besoins de trésorerie et de couvrir une partie des risques liés à l'échange. Mais ils ne sont qu'un maillon de la chaîne : inspecteurs, assureurs, transporteurs, douaniers… interviennent également sur cette chaîne afin de sécuriser l'échange.

Les technologies de registre distribué permettent à ces acteurs de digitaliser cette chaîne, chacun y apportant son information tout en ayant la garantie qu'aucun membre, ni même un administrateur de l'ensemble, ne pourrait venir la corrompre. En revanche, la signature électronique certifiant cette information devient un élément engageant vis-à-vis des autres acteurs de la chaîne. De cette garantie naît la confiance nécessaire à cette collaboration, à ce partage d'informations et à la traduction réelle de l'exécution digitale de la transaction (paiement contre transfert de propriété, par exemple).

---

(1) La'Zooz et Arcade City sont des projets qui visent à utiliser la blockchain *pour « désintermédier » les plateformes de type Uber. Le chauffeur et le passager sont mis en relation sans passer par une plateforme centralisée qui fixe notamment le prix de la course.*

(2) Le Trade Finance *consiste, pour une banque, à financer une marchandise pendant la phase où celle-ci est transférée du vendeur à l'acheteur (par exemple, par bateau). Le formalisme (passages en douane, dépôt dans les entrepôts, connaissement…) y est très important.*

Les entreprises viendraient sur ces plateformes afin d'obtenir soit une réduction de coût par rapport à une formule sécurisée sous le format actuel avec recours à un tiers de confiance, soit un surplus de sécurité, de traçabilité de leur transaction et de sécurisation de l'exécution des paiements, et ce, pour un coût comparable au coût actuel. Elles pourraient à terme accéder, par ce biais, à une *market place* de services de financement et de couverture de divers risques.

Focus sur la titrisation : une synthèse des bénéfices des technologies de registre distribué (DLT)

Le financement de l'économie (dite « réelle ») est effectué massivement *via* les créances commerciales. Pour mémoire, une créance commerciale est la matérialisation dans le bilan d'une entreprise d'une prestation effectuée par un fournisseur, mais non encore payée par le client. De nombreuses entreprises se financent majoritairement grâce à leurs dettes commerciales.

Aujourd'hui, la créance commerciale est peu standardisée (gestion des conflits, gestion des paiements, identification des clients…), ce qui rend cet actif peu liquide. Il est possible, pour une entreprise, de vendre cet actif (*via* la titrisation, l'affacturage ou le *forfaiting*) afin d'obtenir rapidement des liquidités. Mais le coût de cette vente est élevé en raison :

- de la nécessité, pour la banque qui finance de connaître l'acheteur et le vendeur ;
- de la nécessité, en général, de connaître les procédures de recouvrement et de litige entre l'acheteur et le vendeur ;
- du mode de calcul du prix d'achat et de la structure de ce prix (par exemple, paiement différé du prix en fonction de la performance du portefeuille acheté).

Le calcul du prix d'achat est soit très simple, mais, dans un tel cas, il n'est pas très efficace (en raison notamment de l'anti-sélection), soit complexe (auquel cas il nécessite un tiers de confiance pour le valider).

La créance commerciale apparaît donc comme étant un très bon candidat pour l'utilisation de la *blockchain*, qui permettrait :

- de standardiser la créance pour la rendre aussi liquide que possible ;
- d'assurer un suivi simplifié des créances pour l'ensemble des parties prenantes ;
- de simplifier la procédure de transfert ;
- de limiter les coûts de structure *via* une réduction du nombre des intermédiaires et des tiers de confiance ;
- d'effectuer un calcul fin du prix d'achat au sein d'un *smart contract*, qui limiterait les risques d'anti-sélection tout en maximisant le prix d'achat pour le vendeur ;
- d'optimiser la fréquence des paiements : aujourd'hui, une opération de titrisation classique prévoit un transfert par mois, ce rythme pourrait passer, *via* une DLT, à un virement quotidien.

Des prototypes permettant de créer un environnement propice au transfert simplifié des créances au sein de la *blockchain* ont déjà été mis en œuvre, dont l'un a montré que la *blockchain* pourrait supporter un *smart contract* relativement sophistiqué afin de calculer le prix de cession de manière fine, et ce, sans l'intermédiation d'un tiers de confiance explicite. Une prochaine étape devrait être de convaincre des entreprises partenaires de mettre en place l'ensemble du processus. De nombreuses questions juridiques restent en revanche ouvertes à ce stade, et nécessitent d'être traitées en parallèle.

Des questions demeurent…

Lorsqu'Elon Musk s'est entendu expliquer que l'accélération de son premier concept d'Hyperloop tuerait probablement le passager, il a répondu : "*It's an issue* [3]", mais il n'a pas renoncé pour autant. Aujourd'hui, de nombreuses questions restent pendantes autour de l'exploitation de la technologie *blockchain*.

La « scalabilité » en est une : il faut faire en sorte que les crypto-monnaies puissent être échangées dans les mêmes volumes de transaction que leurs grandes sœurs les monnaies fiduciaires sans que soient détériorés les mécanismes qui en assurent la sécurité. Certaines DLT proposent d'utiliser des méthodes de consensus plus efficaces, mais celles-ci ne conservent leur avantage que pour un nombre limité de participants.

Le seul mécanisme « clé publique/clé privé » ne peut garantir l'anonymat de l'utilisateur. En effet, on peut imaginer que dès lors que l'on disposerait d'un nombre de transactions suffisant, des « *patterns* » apparaissent permettant d'établir un lien entre les transactions digitales d'une *blockchain* et les contreparties réelles intervenant sur celle-ci. La police danoise a ainsi été en mesure, à plusieurs reprises, de faire condamner des trafiquants se faisant payer en bitcoins pour échapper aux contrôles de la lutte anti-blanchiment [4]. Il faut donc imaginer une couche supplémentaire renforçant cette anonymisation afin de garantir la confidentialité des transactions.

La gestion des données est un autre élément clé. Les *blockchains* publiques ne garantissent pas la confidentialité des données stockées. Il appartient donc, de prime abord, de définir si des données peuvent apparaître en clair dans les *smart contracts* (si, par exemple, il est impossible de les interpréter…) et d'identifier celles qui ne pourront pas être stockées sans se retrouver en infraction avec les réglementations en vigueur. Enfin, pour les données restantes, il convient de prévoir des mécanismes de cryptage permettant aux seules contreparties concernées de déchiffrer les données les concernant. Selon les cas, certaines DLT ont embarqué ces préoccupations très tôt dans leur développement et ont intégré les mécanismes

(3) « C'est [effectivement] un problème. »
(4) Source : https://thenextweb.com/eu/2017/02/21/danish-police-hunt-down-criminals-using-bitcoin/?utm_source=social&utm_medium=feed&utm_campaign=profeed#.tnw_r146Uuzn

répondant à ces problématiques. Il nous appartient donc d'être extrêmement vigilants dans le choix de la technologie à utiliser, en fonction du cas d'usage envisagé.

Conclusion

Les promesses de la *blockchain* semblent aujourd'hui se confirmer, sans pour autant s'être pleinement concrétisées à ce jour. La technologie doit encore mûrir de façon à répondre aux inquiétudes qu'elle suscite. Le consensus par *proof of work* a montré ses limites (notamment en matière de « *scalabilité* ») et ses successeurs (qu'il s'agisse de la *proof of stake*, de l'insoluble problème des généraux byzantins ou du très prometteur Algorand) doivent encore faire leurs preuves. C'est dans la poursuite des expérimentations et dans une collaboration des BFI élargie à leurs clients et aux autres acteurs de leurs chaînes de valeur que la solution émergera pour le bénéfice de l'ensemble des parties prenantes de ces réseaux d'un type nouveau.

Comment La Poste, acteur de confiance séculaire, aborde-t-elle la *blockchain*, avec l'appui de l'IRT SystemX ?

Par Alain ROSET*
La Poste
et François STEPHAN*
Directeur général adjoint en charge du développement et de l'international de l'Institut de recherche technologique (IRT) SystemX

D'aucuns prédisent que la *blockchain*, nouvelle technologie de rupture, permettra une profonde mutation des tiers de confiance rendue possible par la technologie numérique et la puissance de la multitude. Aux yeux de certains, la *blockchain* semble avoir le pouvoir non seulement de modifier radicalement des modèles économiques historiques établis depuis des décennies ou des siècles, mais aussi de bousculer des modèles économiques très récents (eux-mêmes déjà en rupture). Opérateur historique de confiance depuis des siècles, La Poste renforce depuis plusieurs années sa présence sur Internet et a lancé des services numériques de confiance, confirmant ainsi son rôle de tiers de confiance aussi bien dans l'univers physique que dans l'univers numérique. Le groupe postal français investit depuis 2014 dans la *blockchain* et a décidé, en 2016, de s'associer à l'IRT SystemX, un institut de recherche associant compétences industrielles et académiques, afin d'accélérer son cycle d'innovation s'appuyant sur cette technologie.

Introduction

L'informatique a marqué les dernières décennies de son empreinte, transformant la société et bouleversant certains secteurs économiques. Depuis les premiers calculateurs électroniques apparus au milieu du XX^{e} siècle et leur première formalisation par Alan Turing, plusieurs vagues technologiques ont structuré les développements et Internet révolutionne les échanges entre les individus en permettant la création et la publication d'informations portées par des terminaux toujours plus variés et nombreux.

Avec sa première application de crypto-monnaie bitcoin lancée en 2009, la technologie de la *blockchain* apparaît en 2017 porteuse de nouveaux facteurs déterminants au service de l'innovation numérique : la désintermédiation, la transparence, l'immuabilité, la disponibilité et la sécurité, préfigurant ainsi une nouvelle génération de services de confiance.

Face à ces mutations rapides, l'opérateur postal français doit être à même de comprendre ces évolutions pour adapter ses offres et ses *process*, tout en gardant ses valeurs historiques capitalisées au fil du temps.

La Poste : un grand groupe historique

C'est dans ce cadre particulièrement bouleversé qu'évolue le groupe La Poste, qui est chargé depuis six siècles de porter des messages, dans un premier temps dans le seul intérêt du roi, puis, à partir du règne d'Henri IV, pour des clients privés. La Révolution française impose, par une loi adoptée en 1791, le secret et l'inviolabilité des correspondances. La neutralité de l'opérateur, la préservation de la vie privée et du secret du contenu des correspondances, comme celle des « métadonnées » associées, sont ainsi institutionnalisées et traduites en procédures internes, dont fait partie le « serment du facteur » que doit prononcer tout employé du service lors d'une cérémonie solennelle, et ce, depuis 1790.

C'est ainsi qu'une confiance envers les prestations de l'opérateur postal s'est rapidement installée au sein de la population française, assurant le déploiement de nouveaux produits : des produits d'échanges financiers (mandats) ont été ainsi lancés avec succès dès le début du XIX^{e}

** Les propos tenus dans cet article n'engagent que les auteurs et en aucun cas le groupe La Poste.*

Photo © Jean Vigne/KHARBINE-TAPABOR

Timbre commémoratif français à l'effigie de Louis XI (créateur de la poste d'État) créé à l'occasion de la journée du timbre de 1945.

« La Poste, chargée depuis six siècles de porter des messages, s'intéresse désormais à la *Blockchain*. »

siècle ; ils ont été suivis par des produits d'épargne populaire (avec le livret A) pour finalement permettre à La Poste de devenir un véritable opérateur bancaire, en 2006.

Cette confiance du public a aussi porté le développement, dès les années 1970, d'une vente par correspondance (particulièrement active en France) reposant sur une diffusion fiable de catalogues et de plis publicitaires et les échanges des commandes, des paiements et, enfin, des colis entre les entreprises et les particuliers.

Les évolutions technologiques ont été systématiquement intégrées dans l'offre postale et dans les procédures (tant dans les moyens de transport, depuis la poste aux chevaux jusqu'aux vols de nuit et aux véhicules électriques, que dans les techniques de communication, avec la banque à distance, dès 1980, sur Minitel, l'équipement des guichets en ordinateurs individuels en 1984 et celui de tous les facteurs en *smartphones*, en 2012).

L'évolution des technologies de l'information et des technologies sociétales et leurs impacts sur La Poste

Essentiellement centrée sur les processus internes des entreprises, la première vague de déploiement de l'informatique a affecté l'économie des marchés postaux, mais seulement à la marge : les courriers entre entreprises ont intégralement migré vers le courriel, accompagnés en cela par quelques flux structurés de factures (EDI) – mais cette réduction des volumes postaux a été largement compensée par la croissance des flux publicitaires en direction des particuliers. En revanche, à la fin des années 1990, le développement de l'informatique individuelle au domicile des Français, accompagné de l'envol d'Internet, a réussi à remodeler les liens sociaux et à transformer les communications entre les personnes et les entreprises. Cette dernière évolution a commencé à affecter le marché des échanges postaux en réduisant la part des publicités et en transformant les commandes de vente à distance *via* un e-commerce beaucoup plus dématérialisé.

Reposant pour partie sur une distribution postale à domicile, les ruptures économiques affectant le secteur de la presse écrite sont désormais largement visibles. Mais ce modèle de développement technologique basé sur le protocole TCP/IP (qui est très ouvert) a, contrairement aux augures initiaux, conforté les positions des tiers de confiance, des plateformes d'intermédiation bifaces souvent monopolistiques et bien connues sous l'acronyme des « GAFA » (Google, Apple, Facebook, Amazon), qui pallient les défauts natifs du protocole pour fournir des services à valeur ajoutée. Mais les *spams*, les *fake news* et autre *phishing* démontrent tous les jours la fragilité du système technique sous-jacent.

En parallèle, à l'instar du marché des télécommunications, l'économie postale européenne s'est lancée dans une démarche d'ouverture du secteur à la concurrence, obligeant chaque opérateur à engager une profonde réflexion sur sa stratégie à long terme pour anticiper l'arrivée de concurrents (qui *in fine* n'a jamais été avérée) et la dématérialisation progressive des échanges entre les entreprises et les particuliers.

Le groupe postal français a répondu à ces nouveaux défis par une européanisation de son activité de distribution des colis préfigurant l'impressionnante montée en puissance de l'e-commerce et, sur le marché du courrier, par une alternative différente et originale (parmi les opérateurs européens) d'investissement sur l'ensemble de la chaîne de valeur du courrier. Très tôt, la numérisation largement établie de cette chaîne de valeur a judicieusement apporté des compétences nouvelles au groupe en matière de technologies de l'information, et ce, à des fins tant publicitaires que transactionnelles. Ces compétences associées au patrimoine historique et culturel du groupe ont débouché sur un positionnement de tiers de confiance à la fois dans l'univers physique et dans l'univers numérique, en jouant sur les synergies indispensables dans une société pas encore entièrement acquise aux derniers outils technologiques.

La proposition (en 2008) d'un protocole bitcoin, assemblage subtil de briques technologiques issues des recherches en cryptographie et en informatique distribuée, pourrait préparer une nouvelle rupture dans les technologies de l'information induisant une évolution des relations interpersonnelles ou avec des systèmes automatisés complexes.

La *blockchain* est globalement présentée comme une technologie apte à construire une confiance entre des acteurs ne se faisant pas confiance *a priori* (c'est la métaphore des « généraux byzantins »), propre à supporter des transactions, sans pour autant être portée par un tiers qui est lui-même remplacé par la multitude. Un écosystème riche et bouillonnant est en cours d'installation à l'échelle du globe, avec ses *start-ups*, ses financiers, ses développeurs, ses « mineurs » et ses « gourous » décrivant finement la révolution sociétale à venir et débouchant sur un très grand nombre d'expérimentations.

Très rapidement, cette innovation interpelle le positionnement de tiers de confiance du groupe postal français, qui entreprend une veille active pour en cerner les risques et les opportunités qui sont tapis derrière le « *buzz* » et le « *hype* » du phénomène.

Couplé à un réalisme pragmatique issu des contacts quotidiens des facteurs avec la population française, l'aspect polymorphe des concepts innovants (à la fois techniques, financiers, juridiques et organisationnels) induit pour le groupe postal ces premières conclusions (encore provisoires) :

- La notion de tiers de confiance sera moins centrale, dans une *blockchain*, mais elle restera très présente, en périphérie : gestion des identités et des clés d'accès, validation des informations d'entrée aux transactions (notion d'oracle), par exemple ;
- La maîtrise de la confiance par la multitude demandera une période de transition durant laquelle des initiateurs de services (voire des garants ultimes) seront nécessaires ;
- Les dimensions juridiques et les modèles d'affaires doivent donner lieu à des travaux théoriques et pratiques permettant de guider les modalités de diffusion de la *blockchain* hors du champ des seules crypto-monnaies ;
- L'intrication entre la gestion des transactions et celle de la crypto-monnaie sous-jacente ouvre de nouvelles perspectives de modèles d'affaires, tant pour le lancement de *start-ups* que pour le fonctionnement des services eux-mêmes.

La technologie est encore immature (par exemple, les processus de consensus dans un univers distribué sont étudiés depuis les années 1985, l'immuabilité des *smart*

Dates marquantes de l'Histoire de la Poste

1477 Louis XI crée La Poste d'État à l'usage exclusif du roi. Il met en place le système des relais de poste

1603 Henri IV fait de La Poste royale la première poste aux lettres d'État, celle-ci est à la disposition du public

1790 Les employés des Postes doivent faire le serment de respecter le secret des correspondances

1817 La Poste crée le mandat postal, alternative au transport matériel d'espèces

1829 Création du service des lettres recommandées

1849 Création du timbre-poste français à l'effigie de Cérès (ceux-ci sont gravés par Jacques-Jean Barre)

1881 Création du Livret d'épargne et de la Caisse nationale d'Épargne

1881 Création du service des colis

1912 Premier vol postal officiel en France effectué sur un biplan Farman, de Nancy à Lunéville

1918 La Poste crée les chèques postaux

1972 Création du code postal à cinq chiffres permettant d'automatiser le tri du courrier

1984 Premier TGV postal

2000 (août) La Poste lance @laposte.net et offre une adresse gratuite et pérenne à tous les Français. Création de GeoPost, le pôle colis et logistique du groupe La Poste

2003 Lancement du programme de modernisation industrielle Cap Qualité Courrier

2006 La Poste accueille La Banque Postale, qui endosse le statut d'une banque

2010 Le groupe La Poste change de statut pour devenir une société anonyme à capitaux 100 % publics : La Poste S.A.

2016 Premier service de courrier régulier effectué par des drones

contracts imposera une approche par preuve formelle du code) et elle requiert un approfondissement scientifique important grâce auquel la recherche française en informatique pourra conforter sa renommée mondiale en résolvant des cas d'usage pertinents.

Un approfondissement des faiblesses identifiées dans les *blockchains* est à mener, soit afin de les pallier grâce à des nouveautés algorithmiques devant être soigneusement testées, soit afin de les interfacer avec des prestations déjà existantes, et ce, dans des synergies constructives.

Une nouvelle approche de R&D ouverte pour accélérer l'innovation dans le domaine

Pour mener à bien ces travaux, et en complément à notre participation au projet initié par le groupe Caisse des Dépôts (initiative Labchain) qui s'est focalisé sur les domaines de la banque et de l'assurance, il est apparu, pour l'application de *blockchains* dans les autres marchés sur lesquels le groupe La Poste est présent, qu'une partie des tâches pouvaient se dérouler dans un environnement collaboratif s'appuyant notamment sur des équipes universitaires françaises. C'est ainsi que La Poste s'appuie depuis fin 2016 sur l'IRT (Institut de Recherche technologique) SystemX (situé sur le plateau de Saclay) pour une partie de ses travaux de recherche et développement dans ce domaine.

Nouvel acteur de la recherche partenariale et de l'innovation ouverte en France créé en 2012 avec l'appui du Programme des Investissements d'avenir, l'IRT SystemX accélère la transformation numérique de l'industrie française et des collectivités en réunissant les compétences et les technologies de plus de 70 entreprises partenaires (grands groupes, ETI, PME et *start-ups*) et de sa vingtaine de partenaires académiques actifs autour de projets de recherche et développement en ingénierie numérique des systèmes complexes.

L'IRT SystemX a lancé fin 2016, pour une durée de 4 ans, un projet de R&D sur la *blockchain* qui réunit plusieurs entreprises porteuses de cas d'usage, de technologies et de compétences (dont La Poste) désireuses de mutualiser leurs efforts et de partager leurs avancées sur cette innovation de rupture. Le projet associe des acteurs industriels de tailles variées à des chercheurs académiques de l'Université Paris-Saclay, en particulier l'Inria (avec un partenariat avec l'Université de Berkeley, en Californie), Télécom ParisTech, l'Université de Versailles Saint-Quentin-en-Yvelines et les ingénieurs de recherche de l'IRT.

En participant activement (et financièrement) à ce projet, les industriels partagent les bonnes pratiques sur l'innovation par la *blockchain* tout en bénéficiant d'un enrichissement croisé des avancées technologiques entre les différentes applications de la *blockchain* (comme la mobilité, la logistique, l'énergie, les télécommunications, la sécurité, la finance, etc.).

Le développement, au sein de l'IRT SystemX, d'une plateforme expérimentale permettant de modéliser, de simuler et d'évaluer le couplage des technologies de la *blockchain* au travers de cas d'usage innovants est lui aussi de nature à accélérer l'innovation dans le domaine.

Les principaux défis traités par ce projet couvrent le passage à l'échelle d'une *blockchain*, la notion de confiance numérique (*Data Privacy*, cybersécurité de la *blockchain*), les mécanismes de consensus et de validation des transactions, la gouvernance de services s'appuyant sur une *blockchain*, les tests de maturité des briques technologiques de la *blockchain*, l'interopérabilité et l'intégration « *cross-chain* », les modèles économiques, l'acceptabilité sociétale, les aspects juridiques.

Au printemps 2017, l'IRT SystemX a lancé son programme « START@SystemX » en direction des *start-ups* œuvrant au développement de la *blockchain*. Les *start-ups* sélectionnées se voient offrir l'opportunité de valoriser pour elles le potentiel de la *blockchain* en collaborant avec des acteurs industriels et académiques du projet de R&D de SystemX, au travers de sa plateforme de recherche expérimentale.

Conclusion

Il est vraisemblable qu'aux environs de 2020, plusieurs services de confiance reposeront sur des *blockchains*, principalement au sein de consortiums qui s'ouvriront progressivement à des partenaires toujours plus nombreux constituant des grappes de services interconnectés de façon sécurisée. Plusieurs domaines des services postaux pourront être modernisés en s'appuyant sur les avantages des *blockchains* qui apporteront l'unicité des enregistrements, la transparence, l'auditabilité de toutes les opérations et l'immuabilité des informations. Le groupe La Poste aura alors à retravailler son positionnement de tiers de confiance pour s'adapter à cette nouvelle technologie en apportant des réponses aux fragilités du système, à savoir la gouvernance entre toutes les parties prenantes, la capacité du passage à l'échelle, les faiblesses en périphérie de la chaîne centrale, la gestion des identités physiques des utilisateurs, et ce, en s'appuyant sur l'ouverture de certaines réglementations qui conserveront leurs finalités sans imposer des modalités de mise en œuvre trop précises.

Cette vision globale repose sur la mobilisation des ressources scientifiques françaises autour de ces thématiques (que celles-ci se trouvent dans les entités de recherche ou qu'elles soient déjà engagées dans des *start-ups*), que le projet « *Blockchain for Smart Transactions* » de l'IRT SystemX coordonnera.

Souhaitons que grâce à ces compétences le groupe La Poste sache construire de nouvelles offres et intégrer cette nouvelle technologie qu'est la *blockchain*, et ce, au service de l'ensemble des citoyens français.

Le fonctionnement de la *blockchain*

Par Gautier MARIN-DAGANNAUD
Élève-ingénieur à Télécom ParisTech – Institut Mines-Télécom et étudiant en master à l'École polytechnique, actuellement chez Ledgys

La *blockchain* est une technologie profondément disruptive. Pour en saisir le potentiel, il est indispensable de comprendre les bases de son fonctionnement à travers son cas d'usage originel, Bitcoin. Une *blockchain* est un registre distribué, c'est-à-dire partagé entre les acteurs d'un réseau. Comme dans tout registre, il y a des utilisateurs, qu'il faut pouvoir identifier, et des transactions, qui modifient l'état du registre. Cependant, à la différence de l'immense majorité des registres actuels, la *blockchain* fonctionne sans autorité centrale de contrôle. Cela implique de nombreux enjeux et problématiques techniques.

Les plateformes logicielles actuelles (Facebook, Amazon, Uber, banques en ligne) ont toutes un point commun, celui d'être organisées autour d'un acteur central chargé de maintenir leur intégrité et d'assurer leur développement. Cette centralisation a des avantages, notamment en termes de rapidité dans la gestion des conflits et de capacité à monter en charge, mais elle présente également de nombreux inconvénients, comme la censure, le monopole ou la vulnérabilité aux attaques.

La *blockchain* est une technologie permettant de partager une base de données de manière décentralisée, c'est-à-dire entre acteurs ne se faisant pas nécessairement confiance et sans entité centrale de contrôle. Elle rend possible la création d'un nouveau type de plateforme logicielle, les plateformes décentralisées. Pour bien saisir ce changement de paradigme, il est nécessaire de comprendre les bases du fonctionnement de cette technologie.

Comment fonctionne une *blockchain* ? L'exemple de Bitcoin

Les origines

À l'origine, la technologie *blockchain* a été inventée pour permettre la création de la première monnaie numérique décentralisée, le Bitcoin. Bitcoin est un système de paiement digital s'appuyant sur la crypto-monnaie du même nom. Comme dans tout système de paiement, il est nécessaire de tenir à jour un registre des comptes pour pouvoir connaître la balance financière de chaque utilisateur. Dans le monde « réel », ce sont les banques qui tiennent ce registre. Si l'on souhaite envoyer de l'argent à quelqu'un, il faut en faire la requête à la banque, puisque c'est elle qui tient les comptes. On parle d'organisme centralisé. Le principe fondamental de Bitcoin est relativement simple : au lieu que le registre soit maintenu par un seul organisme privé, il l'est de manière décentralisée. En clair, chaque ordinateur (appelé nœud) du réseau contient une copie du registre et aide à le maintenir à jour. Le registre est protégé par cette décentralisation. En effet, même si un ou plusieurs nœuds sont altérés ou détruits, le registre sera conservé tant que subsisteront des nœuds « honnêtes ».

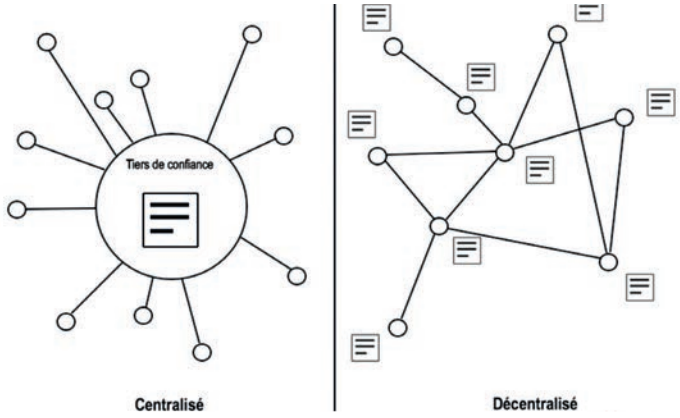


Figure 1 : Deux systèmes de maintien d'un registre : centralisé *vs* décentralisé.

Identifier les utilisateurs

Les utilisateurs du réseau sont identifiés par leur adresse, qui permet aux autres utilisateurs de leur envoyer des bitcoins. À chaque adresse est associée une clé privée. C'est elle qui permet de « débloquer » les fonds. L'adresse est générée en local par l'utilisateur à partir de sa clé privée, et ce, grâce à de complexes fonctions mathématiques, dont il suffit de retenir qu'elles fonctionnent à sens unique. S'il est quasiment impossible de trouver la clé privée associée à une adresse donnée, il est en revanche très facile de trouver l'adresse correspondant à une clé privée.

Pour débloquer les fonds, l'utilisateur n'a pas à communiquer sa clé privée au réseau. S'il le faisait, n'importe quel nœud la recevant pourrait dépenser les fonds associés à l'adresse correspondante. Au lieu de cela, il produit – toujours en local – une signature électronique associée à la transaction qu'il souhaite effectuer. Cette signature électronique prouve que la personne possédant la clé privée

a bien approuvé la transaction. Elle est unique, ce qui signifie qu'elle ne peut pas être réutilisée pour une autre transaction. De plus, la fonction permettant la création de la signature est elle aussi à sens unique. Les nœuds du réseau ne peuvent donc pas deviner la clé privée associée à cette signature.

Le mécanisme de la signature électronique permet donc d'autoriser des transactions sans révéler la clé privée au réseau. Si la signature électronique est un outil indispensable au fonctionnement de Bitcoin, ce n'est toutefois pas l'innovation apportée par la technologie *blockchain*.

Les bases de la *blockchain*

L'innovation de la technologie *blockchain* porte sur le consensus. Plus précisément, il s'agit d'apporter une solution au problème de la double dépense, un problème prépondérant dans tout système décentralisé. Supposons qu'un utilisateur signe et envoie au même moment deux transactions prenant pour point d'entrée le même bitcoin, mais ayant deux destinataires distincts. Certains nœuds recevraient l'une des deux transactions en premier, ce qui invaliderait la seconde, tandis que d'autres effectueraient le processus inverse. À l'échelle du réseau, il y aurait donc un désaccord sur l'état du registre.

Pour pallier ce problème, Bitcoin propose d'enregistrer de manière ordonnée et horodatée les transactions dans une chaîne de blocs avec laquelle chacun des nœuds doit se synchroniser : c'est la *blockchain*. Cette chaîne est unique et permet à tous les nœuds de s'accorder sur l'état du registre. Les blocs contiennent une liste des transactions qui modifient l'état du registre. L'ajout de blocs s'effectue au niveau de chaque nœud. Ainsi, tous les nœuds possèdent une copie à l'identique de la *blockchain* (à quelques subtilités près). Chaque bloc référence le bloc précédent, ce qui forme une chaîne de blocs qui s'étend jusqu'au « *genesis block* », le tout premier bloc à avoir été créé. Pour connaître l'état du registre à un instant donné, il suffit de remonter la chaîne des blocs depuis son origine jusqu'au dernier bloc ajouté avant l'instant considéré.

Le fonctionnement simplifié de la *blockchain*

Après avoir été générée par un utilisateur, une transaction est transmise aux nœuds voisins, puis relayée de pair en pair à travers le réseau. Pour qu'une transaction émise soit valide, il faut que l'utilisateur dispose des fonds requis et que sa signature soit valide. Cependant, une transaction n'est pas finalisée tant qu'elle n'a pas été incluse dans un bloc. De plus, deux transactions concurrentes, c'est-à-dire qui tentent de dépenser les mêmes bitcoins, ne peuvent pas être incluses dans le même bloc. Dans ce système, il est donc impossible d'effectuer une double dépense.

Reste à savoir quel nœud a le droit de créer le prochain bloc. Les nœuds créateurs de blocs sont des nœuds spéciaux que l'on appelle « mineurs ». N'importe quel nœud peut devenir un « mineur », il suffit pour l'internaute de disposer du matériel et du logiciel adéquats. Lorsqu'un mineur reçoit une nouvelle transaction non validée, il la place dans ce que l'on appelle « l'ensemble des transactions non confirmées ». Cet ensemble est propre à

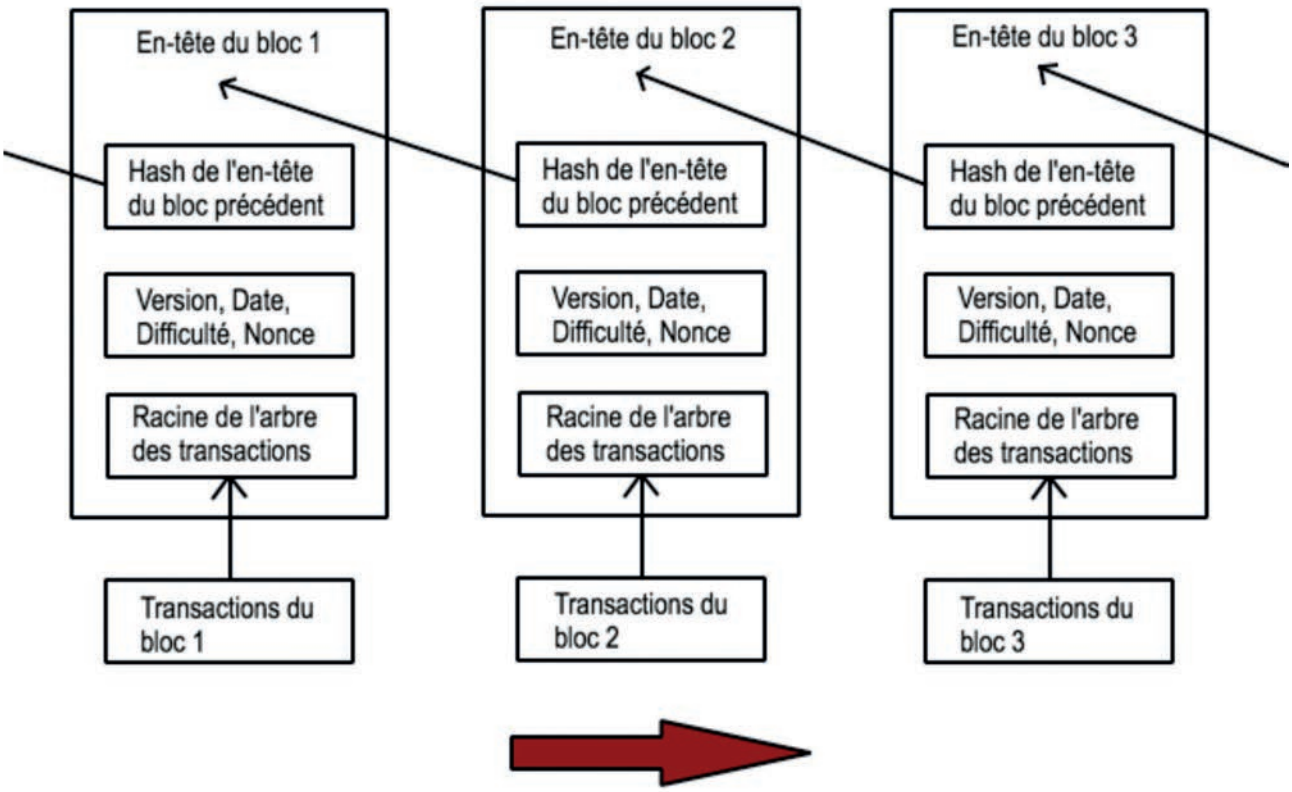


Figure 2 : Fonctionnement simplifié de la *blockchain*.

chaque mineur, il peut différer d'un mineur à l'autre du fait du temps de propagation des transactions sur le réseau. C'est une sorte de liste d'attente pour transactions, celles-ci en sortant une fois qu'elles ont été incluses dans un bloc.

Créer un bloc : la « preuve de travail »

N'importe quel mineur peut collecter un certain nombre de transactions dans sa liste, vérifier leur validité et former un bloc. Cependant, ce bloc ne sera pas validé tant que le mineur n'aura pas produit la « preuve de travail » (*Proof of Work*) associée au bloc considéré. Cette preuve de travail est une donnée difficile à produire, mais facile à vérifier. Sans cette donnée, le bloc ne peut pas être validé par les nœuds du réseau, même si les transactions qui le composent sont valides. Le fait qu'il soit difficile de créer cette donnée permet de décider lequel des blocs créés par les mineurs sera ajouté à la chaîne.

Pour produire cette donnée, les mineurs doivent calculer la valeur d'une fonction prenant pour entrées l'empreinte [1] (également appelée « *hash* ») du bloc précédent, l'empreinte des éléments du bloc actuel et un nombre variable, appelé « nonce ». Les mineurs font varier ce nonce jusqu'à ce que le résultat de la fonction réponde à des conditions prédéfinies par le protocole, notamment à un paramètre nommé « difficulté », qui permet de définir l'étendue des résultats valides. Plus la difficulté est élevée, et plus l'étendue est restreinte, ce qui rend la découverte d'un nonce valide plus compliquée. Il est également important de noter que, là encore, la fonction est à sens unique. Il est donc impossible de prédire à l'avance un nonce qui satisfasse aux conditions du protocole. Ainsi, le seul moyen de trouver un nonce valide est de faire calculer à sa propre machine un très grand nombre de nonces, d'évaluer pour chacun d'entre eux la valeur de la fonction et d'en vérifier la validité. Pour un seul nœud, il faudrait en moyenne plusieurs années pour trouver un bloc valide. À l'échelle du réseau, la difficulté est établie de telle sorte qu'en moyenne 10 minutes sont nécessaires pour qu'un nœud trouve un bloc valide. Si la preuve de travail est difficile à produire, elle est en revanche très facile à vérifier. Pour vérifier si une preuve est valide, il suffit d'évaluer la valeur de la fonction pour le nonce donné. On peut faire une analogie avec la combinaison d'un cadenas : trouver la combinaison par itérations est un processus très long, mais il est en revanche très facile de vérifier si une combinaison ouvre le cadenas – dans notre cas, si elle est valide.

La propagation des blocs

Une fois la preuve trouvée, le nœud « gagnant » ajoute son bloc à la chaîne. On dit qu'il a « miné » le bloc. Il reçoit en compensation une somme fixe déterminée par le réseau (12,5 bitcoins, aujourd'hui), ainsi que les éventuels frais de transaction. Bitcoin encourage donc les mineurs à entretenir le réseau en les récompensant par une rémunération. C'est par ailleurs de cette manière que des bitcoins sont introduits dans l'écosystème.

Ensuite, le mineur transmet le bloc au reste du réseau. Tous les nœuds qui le reçoivent vérifient la validité des transactions du bloc, ainsi que la preuve de travail, puis ajoutent le bloc à la chaîne. Si le nœud est un mineur en train de chercher un bloc valide, il doit reprendre le processus de création de bloc à partir de ce nouveau bloc créé (rappelons que tout bloc pointe sur le précédent). Il est possible qu'un nœud du réseau reçoive des blocs – ou des successions de blocs – valides concurrents. Dans ce cas, la règle est de toujours prendre la chaîne la plus longue comme référence.

Cette règle implique que pour qu'un attaquant fasse accepter aux nœuds du réseau sa version de la chaîne, il doit être en mesure de produire une chaîne de blocs valides plus longue que celle sur laquelle travaillent tous les autres mineurs « honnêtes ». En d'autres termes, il doit posséder plus de 50 % de la capacité de calcul du réseau. C'est ce que l'on appelle une « attaque 51 % ». Le réseau est donc d'autant plus sécurisé que la puissance de calcul combinée des mineurs est élevée. Notons tout de même qu'une telle attaque ne permettrait pas aux attaquants de voler des bitcoins, puisque ces derniers sont protégés par le mécanisme de signature digitale. Ils ne pourraient effectuer, tout au plus, que des doubles dépenses ou des dénis de service.

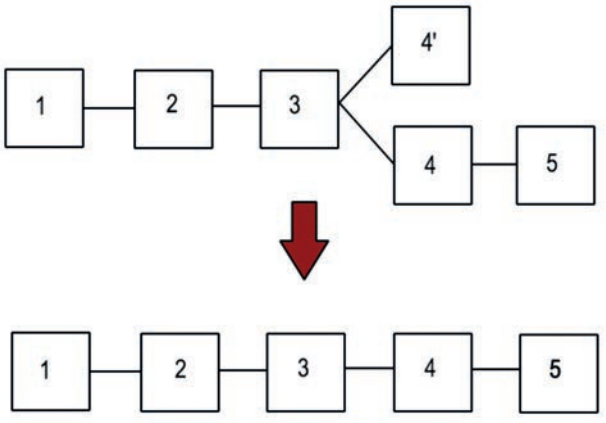


Figure 3 : Le basculement vers la chaîne de blocs la plus longue.

Au-delà de la monnaie

L'Internet de la valeur

Au départ, l'innovation technologique de la chaîne de blocs avait été éclipsée par son application première, la monnaie bitcoin. Cependant, il n'a pas fallu longtemps pour que l'on prenne conscience de son potentiel. Les bitcoins ne sont qu'une suite de 0 et de 1, ils peuvent être dupliqués sans effort. Comment s'assurer de la va-

(1) Une empreinte, ou hash, *est le résultat d'une fonction de hachage appliquée à une donnée initiale. La fonction de hachage est une fonction à sens unique. Son résultat est généralement un nombre hexadécimal (= de base 16) de taille fixe (256 bits, par exemple). Pour une même donnée initiale, on obtiendra toujours la même empreinte. En revanche, il est quasiment impossible de déterminer la donnée initiale à partir de son empreinte.*

leur d'un actif que l'on peut dupliquer indéfiniment ? Dans le cas de la monnaie fiduciaire, on a recours à des autorités centrales qui maintiennent l'intégrité du registre. Dans le cas de Bitcoin, c'est la *blockchain* qui assure la non-multiplication de la monnaie. Le principal intérêt de la *blockchain* est sa capacité à donner de la valeur à des actifs numériques, et ce, sans avoir recours à une autorité centrale.

Colored Coins et *Smart Contracts*

Les actifs numériques s'étendent au-delà de la monnaie. Par exemple, le protocole *Colored Coins* permet de représenter des actifs réels (actes de propriété, actions, obligations) *via* la *blockchain* Bitcoin. D'autres *blockchains* ont été créées pour faciliter la création de *tokens* (des jetons). Par exemple, Ethereum est une *blockchain* permettant le déploiement des contrats intelligents (*smart contracts*). Ces contrats sont des programmes dont l'exécution est assurée par les nœuds du réseau. Ils permettent d'automatiser la logique contractuelle et de la transposer aux actifs numériques. Avec Ethereum, il est possible de déployer une infinité d'actifs numériques valorisés par la *blockchain* et d'en automatiser la gestion grâce à des contrats intelligents. Une fois un tel contrat déployé sur le réseau, il est impossible d'en censurer l'exécution lorsqu'il est appelé, ni de l'annuler. Seul un consensus mondial de l'ensemble des acteurs du réseau – mineurs, développeurs, échanges et utilisateurs – peut permettre de revenir sur l'exécution d'un contrat. Cela fait de la *blockchain* le système le plus résistant à l'intervention d'un tiers parti que nous ayons jamais eu.

À nouvelles plateformes, nouveaux enjeux

Aujourd'hui, il existe des centaines de *blockchains* pour des centaines d'usages différents. De nombreuses plateformes décentralisées sont en train de voir le jour. Elles sont non propriétaires et *open source*, ce qui implique de nombreux changements en matière de répartition de la valeur. Les crypto-monnaies jouent un rôle très important dans cette répartition. En général, une crypto-monnaie spécifique à une plateforme est créée lors de son lancement. Elle est répartie selon les règles programmatiques qui régissent la plateforme, règles qui peuvent elles-mêmes évoluer conformément aux mécanismes de gouvernance spécifiques à la plateforme, de sorte que la répartition de la monnaie tende vers un optimum. Dès lors, chaque acteur de la plateforme est récompensé en fonction de son apport à l'écosystème, dans une logique de libre marché. Cela contraste avec les plateformes existantes, dans lesquelles l'autorité centrale est chargée de répartir la valeur et les responsabilités.

Des points de centralisation existent encore à l'heure actuelle. Notamment les plateformes d'échange de crypto-monnaies sont, dans leur immense majorité, opérées par des organisations centralisées. Cependant, des échanges décentralisés sont en cours de développement. Il existe même des projets visant à connecter les *blockchains* entre elles, et ce, de manière décentralisée. Ce serait là entrer dans un monde de plateformes interopérables sans friction.

Cependant, de nombreux défis d'ordres technique, légal et organisationnel restent à relever – avant de pouvoir y arriver.

Références sur la Toile

http://bitcoin.stackexchange.com/questions/22/is-it-possible-to-brute-force-bitcoin-address-creation-in-order-to-steal-money

https://www.reddit.com/r/BitcoinBeginners/comments/3eq3y7/full_node_question/ctk4lnd

https://bitcoin.org/en/developer-guide#block-chain

http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

https://github.com/ethereum/wiki/wiki/White-Paper

https://en.bitcoin.it/wiki/Main_Page

http://bitcoin.stackexchange.com/questions/11054/understanding-spv-simple-payment-verification

Blockchains et *smart contracts* : premiers retours d'expérience dans l'industrie musicale

Par Christophe WAIGNIER
Directeur des ressources et de la stratégie, Société des auteurs, compositeurs et éditeurs de musique (Sacem)

L'industrie musicale est depuis maintenant plus de quinze années au cœur de la transformation numérique. Dans ce contexte, les *blockchains* suscitent naturellement de nombreux débats au sein de la communauté artistique et des acteurs de l'industrie musicale, aux États-Unis comme en Europe. À l'initiative de *start-ups*, mais aussi d'acteurs plus traditionnels comme la Sacem, des expériences concrètes commencent à voir le jour. Les premiers résultats obtenus suscitent l'intérêt, ouvrant de nouvelles perspectives de collaboration entre les différents acteurs du secteur. Mais ces technologies émergentes restent cependant encore trop fragiles pour représenter, à court terme, un réel levier d'accélération de la transformation numérique du secteur.

Depuis plus de quinze ans, la culture et ses industries sont au cœur de la transformation numérique. Véritable pionnier, le secteur de la musique a largement contribué à cette transformation. Le numérique a introduit de nouveaux usages et entraîné une dissémination des contenus culturels ainsi que l'explosion de leur accessibilité, quelle que soit la localisation du consommateur dans le monde.

Pour comprendre quels sont les enjeux technologiques que nous devons relever et réfléchir sur les potentialités des *blockchains*, il est nécessaire d'avoir quelques notions sur notre activité.

Derrière une œuvre musicale, il y a toujours des créateurs (auteurs et compositeurs), mais également des éditeurs (un éditeur principal et des sous-éditeurs dans d'autres pays) qui développent la carrière des auteurs dont ils ont la charge et qui assurent l'exploitation commerciale de leurs œuvres. Par ailleurs, une œuvre se doit d'être interprétée et de donner lieu soit à des enregistrements financés par un producteur phonographique, soit à des exécutions publiques financées par un producteur de spectacles. Les enregistrements peuvent être reproduits sur divers supports (CD ou vinyles) et vendus. Ils peuvent aussi faire l'objet de diffusion (à la radio, à la télévision, dans les magasins, etc.) ou encore être proposés sous une forme dématérialisée (au format MP3, par exemple).

Nous répertorions près de 20 millions d'œuvres musicales dans notre base de documentation et nous évaluons à près de 200 millions les produits numériques de musique enregistrée mis à la disposition de l'ensemble des consommateurs de musique dans le monde, *via* des millions de diffuseurs (stations de radio, chaînes de télévision, salles de spectacles, magasins, plateformes Internet, etc.). Cet écosystème est par nature très décentralisé, il reflète la diversité des cultures, des genres musicaux et des pratiques de consommation de la musique. La technologie doit être une solution qui facilite la préservation de cette diversité et non un outil imposant une quelconque standardisation.

Notre objectif à la Société des auteurs compositeurs et éditeurs de musique (Sacem) est d'assurer la gestion économique de cet ensemble pour le compte des auteurs, des compositeurs et des éditeurs. Nous effectuons 700 000 contrats de diffusion de musique par an, pour lesquels nous encaissons plus de 900 millions d'euros. Nous traitons 6 milliards de lignes d'information sur les diffusions de la musique afin de répartir cette somme sur environ 2 millions d'œuvres au profit de 300 000 auteurs, compositeurs et éditeurs de musique. Même si, bien entendu, les volumes d'informations à traiter ont considérablement augmenté, telle est pour l'essentiel la finalité de notre action, et ce, depuis notre création en 1851… La numérisation de notre écosystème a d'ores et déjà beaucoup changé nos processus et notre organisation, mais nous ne sommes qu'au début de ce grand mouvement de transformation.

Pourquoi (et comment) introduire les *blockchains* dans notre écosystème ?

Il est intéressant de constater qu'une réflexion sur les *blockchains* dans la musique a commencé à émerger outre-Atlantique, du côté de Boston au *Berklee College of Music*, où l'on forme les plus grands musiciens de jazz de la planète. Il est quasi certain que ces jeunes intellectuels de la musique fréquentent les mêmes bars que les étudiants du *Massachusetts Institute of Technology* (MIT). De ces rencontres informelles est née une initiative pilotée par les étudiants du *Berklee College*, qui a été baptisée « *Rethink Music* » et à laquelle la Sacem a participé, une initiative qui avait pour but de réfléchir « *out of the box* » sur l'industrie musicale afin d'imaginer un système de rémunération plus satisfaisant pour les artistes. Très vite ces discussions ont eu pour sujet principal les *blockchains*.

Mais essayer d'envisager l'introduction d'une technologie aussi révolutionnaire que celle des *blockchains,* c'est se replacer dans le contexte du démarrage de l'Internet pour tenter de dresser un inventaire d'un champ infini de possibles.

Par quoi commencer ? Qui doit être à l'initiative ? Comment coordonner nos actions ?

Même si les artistes sont habitués aux exercices créatifs, l'industrie musicale a du mal à dépasser le stade des forums de discussions et des conférences sur le sujet des *blockchains*. Actuellement, le principal espace de discussions et d'échanges à ce sujet, qui regroupe l'ensemble des acteurs de la chaîne de valeur s'appelle l'*Open Music Initiative*, que pilote également le *Berklee College*. Il regroupe (là encore, aux États-Unis) un ensemble d'artistes et d'éditeurs, ainsi que certaines majors de la musique et de la gestion collective représentées par la Sacem et par des plateformes comme Spotify ou YouTube. Mais pour le moment, rien de vraiment concret n'a encore émergé de ces discussions auxquelles participent un trop grand nombre d'interlocuteurs dont les points de vue ont du mal à converger sur un objectif commun.

Au-delà de forums qui ont pour but de faire un utile travail de sensibilisation auprès de la communauté des acteurs du monde de la musique, certaines initiatives plus concrètes commencent à voir le jour.

On peut ainsi identifier une première catégorie d'initiatives qui regroupe des acteurs partageant le même objectif, celui de proposer à un nombre limité d'artistes une solution de distribution digitale de musique « *direct to fans* », sans passer par l'intermédiaire des plateformes de services existantes (telles que Spotify ou iTunes, par exemple). C'est le cas d'Ujo Music, qui a développé une solution de distribution pour l'artiste Imogen Heap permettant de mettre à la disposition de ses fans son dernier album, avec la possibilité pour eux d'acheter sa musique au moyen de bitcoins. Derrière Ujo Music, on retrouve la société Consensys, qui commercialise des solutions *blockchain* (à but très lucratif !) partout dans le monde et qui est affiliée au consortium technologique Etherium. À noter, également, l'initiative récente de Benji Rodgers, patron fondateur du label digital américain *Pledge Music*, qui vient de démarrer *Dot Blockchain Music* avec pour ambition de proposer à l'industrie musicale une solution totalement ouverte de distribution numérique. On peut citer également, dans le même registre, les projets *Revelator, Blokur Internet Music* ou *Stems*.

En résumé, ces démarches proposent essentiellement de remplacer les technologies qui sous-tendent actuellement la distribution numérique de la musique par les *blockchains*, en se présentant comme des intermédiaires uniques de la chaîne de valeur. Mais loin de tenir leur promesse de supprimer les intermédiaires, ces nouveaux acteurs les concentrent. Ils se prétendent être capables de remplacer des acteurs ultraspécialisés indispensables dans un secteur aussi mature que la musique. Ces initiatives sont d'ailleurs souvent portées par de nouveaux entrants ayant plus souvent pour objectif de faire parler d'eux que de proposer une amélioration pérenne pour l'ensemble de l'industrie.

Il existe une deuxième catégorie d'initiatives qui regroupe des démarches bien différentes : au lieu de s'attaquer à l'ensemble de la chaîne de valeur en ayant pour objectif de tout changer, d'autres acteurs proposent d'évaluer la capacité des *blockchains* à régler un problème spécifique de l'industrie musicale. Ainsi, les Canadiens de la SOCAN et les Finlandais de Teosto proposent des plateformes de médiation permettant à un artiste-interprète de contractualiser avec une salle de concert et de déclarer l'ensemble des chansons qu'il va jouer sur scène afin de permettre la rémunération de l'éditeur, de l'auteur et du compositeur, ainsi que celle de l'ensemble des intervenants sur l'événement (en ayant probablement l'idée de commercialiser par la suite les billets auprès des spectateurs sur la même plateforme).

La société de gestion de droits Allmade, qui opère surtout dans des pays africains, propose un système de boîtier à installer dans des lieux sonorisés permettant l'identification des titres diffusés et de produire un *reporting* des diffusions à destination des sociétés de gestion collectives pour pouvoir aboutir à une répartition des droits plus juste. Ce processus totalement géré par des *blockchains* permet une grande traçabilité des œuvres et assure un maximum de transparence sur leur diffusion.

De son côté, la Sacem a choisi une approche pragmatique en décidant de développer un premier outil sous la forme d'une *proof of concept* (POC). Il s'agissait de rester réaliste en adoptant une approche pas à pas qui soit en mesure de créer rapidement de la valeur. Ainsi, contrairement à certaines initiatives *blockchain* qui montent un produit dans leur coin, nous avons choisi, quant à nous, de nous associer avec deux des plus grandes sociétés d'auteurs du monde afin de rester fidèles à l'esprit des *blockchains*, qui est de permettre le partage entre plusieurs acteurs, mais également de prendre en compte la dimension internationale du problème. C'est ainsi que rejoints par la *PRS for Music Limited*, notre homologue anglaise, et par l'*Ascap* (*American Society of Composers, Authors, and Publishers*), notre homologue américaine,

nous avons décidé d'unir nos forces pour nous concentrer, dans un premier temps, sur l'un des principaux sujets de discussion de notre industrie, à savoir l'absence d'un registre partagé où se trouverait le lien entre une œuvre et l'ensemble des différentes interprétations enregistrées qui en sont issues.

Documenter ces liens est un des savoir-faire très spécifiques des sociétés d'auteurs. Mais en dépit de la coopération qui existe entre elles, rien n'avait encore été mis en place pour partager ces informations. Par chance, les œuvres comme les enregistrements sont estampillés de codes internationaux normés reconnus par l'Organisation internationale de normalisation ISO : les ISWC (*International Standard Musical Work Codes*) et les ISRC (*International Standard Recording Codes*). Ainsi, étudier le lien entre une œuvre et ses interprétations enregistrées établi par une société spécialisée revient à étudier le lien existant entre deux codes, ce qui est beaucoup plus simple.

Notre choix technologique s'est porté sur Hyperledger, une plateforme *open source* de développement initiée en décembre 2015 par la fondation Linux qui a fait le choix d'un développement essentiellement en langage Go. L'intérêt de cette technologie est de permettre d'avoir un registre partagé pouvant dérouler des *smart contracts* tout en garantissant l'authentification de ses utilisateurs. Cette technologie permet ainsi de s'affranchir de certaines contraintes des *blockchains* publiques, notamment en matière de temps de calcul.

La première phase du projet s'est achevée à la mi-mars 2017, faisant de la Sacem la première société d'auteurs à coder concrètement une application basée sur les *blockchains*. Cette première phase a clairement démontré l'intérêt fonctionnel d'un enrichissement mutuel entre diverses sociétés d'auteurs, puisque près de 80 % des appariements auteur-interprète étaient détenus par une seule des 3 sociétés impliquées. Elle a aussi mis en avant les difficultés d'identification auxquelles chaque société doit faire face (2 % de conflits répertoriés trouvant toujours une solution, mais nécessitant encore une fastidieuse analyse manuelle au vu du nombre des cas possibles).

D'un point de vue technique, l'immaturité de la technologie a clairement été identifiée comme un frein à son déploiement rapide (un constat classique fait au démarrage de toute nouvelle technologie), comme ce fut le cas pour le langage Java ou Lucene, une bibliothèque en *open source*. Mais son potentiel reste entier notamment grâce à sa capacité à faire travailler ensemble des acteurs aux intérêts divers, où chacun peut en tirer un bénéfice non négligeable tout en faisant progresser l'ensemble.

Afin de progresser dans cette expérimentation, il nous revient maintenant d'entrer dans une seconde phase en démontrant que les *blockchains* sont à même de bien répondre aux enjeux de volumétrie de l'industrie musicale, mais également d'intégrer plus facilement que les autres technologies des acteurs ayant des problématiques complémentaires. Il conviendra également de s'assurer de la flexibilité du système pour identifier des modes de résolution de conflits plus automatiques et de compléter la promesse des *blockchains* par celle de l'intelligence artificielle, tout en assurant des interfaces adéquates répondant plus facilement aux besoins de chacun des métiers impliqués.

Photo © Florence Duran/SIPA

Le siège de la SACEM à Neuilly-sur-Seine (département des Hauts-de-Seine).

« Dans un univers hypothétique où tout le monde utiliserait la *blockchain* pour gérer ses œuvres, contractualisant directement avec des diffuseurs (*online*, *on air* ou *on stage*), il y a fort à parier que des créateurs se regrouperaient pour mieux gérer ces sujets et défendre efficacement leurs droits face aux grands acteurs de l'Internet. »

Ces derniers défis restent les plus importants. En effet, derrière cette technologie, il n'y a pas d'intelligence et il convient, dans le secteur qui est le nôtre, de définir des règles afin d'assurer l'intégrité des données qui sont utilisées et leur présentation et ainsi d'éviter le « *garbage in – garbage out* » qui pourrait rapidement en découler, créant plus de problèmes qu'il n'en résoudrait. À ce stade, nous ne pensons donc pas que la *blockchain* puisse suffire à elle seule à régler les problèmes de notre industrie. La nécessité de trouver un nouveau mode de gouvernance de ce genre de projet doit être définie afin d'impliquer un maximum d'acteurs, sans pour autant retomber dans les travers d'une base centralisée. Nous travaillons actuellement à ces questions afin de nous assurer d'avoir, au final,

un système pérenne et économiquement viable, qui soit certes ouvert, mais aussi suffisamment organisé.

En résumé, dans un monde où les données gagnent chaque jour de la valeur et où le premier réflexe est de se demander à qui ces données appartiennent, sur la *blockchain*, il s'agit de trouver le compromis indispensable pour amener les industriels à contribuer à l'atteinte de la masse critique nécessaire pour que cette solution fasse autorité auprès du groupe des contributeurs et des utilisateurs.

Ainsi la *blockchain* reste une technologie émergente, qu'il convient d'étudier, mais sans se précipiter. Les fantasmes faisant de la *blockchain* LA réponse à tous les problèmes de transparence et de traçabilité sont fort éloignés de la réalité d'une l'industrie qui, certes, se démocratise énormément, mais qui est également, et surtout, constituée de professionnels extrêmement pointus sur leurs métiers – des professionnels que la *blockchain* ne saurait remplacer.

Ainsi, dans un univers hypothétique où tout le monde utiliserait la *blockchain* pour gérer ses œuvres, contractualisant directement avec des diffuseurs (*online*, *on air* ou *on stage*), il y a fort à parier que des créateurs se regrouperaient pour mieux gérer ces sujets et défendre efficacement leurs droits face aux grands acteurs de l'Internet.

En bref : si la Sacem n'existait pas, il faudrait… l'inventer !

Objets d'art : les enjeux de la *blockchain*

Par Jurgen DSAINBAYONNE
Fondateur de Seezart

Le marché de l'art a entrepris depuis quelques années sa mutation digitale. Plusieurs forces s'exercent, à savoir : l'impact des nouvelles technologies, un renouvellement générationnel du profil des collectionneurs et, enfin, la crise de 2008 qui, ayant mis à mal le marché des rendements obligataires, a eu pour effet de renforcer la vision de l'œuvre d'art en tant qu'actif financier. Cette digitalisation met également en lumière les failles d'un système considéré, à tort ou à raison, comme opaque et marqué par l'entre-soi. De nombreux scandales éclatent, remettant en cause les droits d'auteur, la légalité, l'authenticité, la provenance et jusqu'à la valeur même des œuvres d'art.
C'est dans ce contexte que la technologie *blockchain*, de par ses propriétés intrinsèques, peut renforcer et garantir une confiance numérique et répondre aux enjeux d'un marché en pleine mutation.

Le 30 novembre 2011, la Galerie Knoedler, la plus ancienne galerie d'art des États-Unis, à la réputation irréprochable, fermait brutalement ses portes. Cette institution presque bicentenaire s'était retrouvée au cœur d'un scandale du fait de la vente d'une série d'œuvres prétendument « rarissimes » de l'expressionnisme abstrait, pendant une quinzaine d'années – des « œuvres » qui se sont révélées être des faux.

D.R.

Illustration 1 : La galerie d'art Knoedler, à New York.

Leur authenticité, mais plus encore leur provenance furent fortement contestées. Ce fut notamment le cas pour un tableau de (ou plutôt attribué à) Jackson Pollock, que deux des plus grandes maisons d'enchères – Sotheby's et Christie's – refusèrent de mettre en vente.

Cette affaire, parmi beaucoup d'autres, illustre l'une des problématiques centrales du marché de l'art : l'établissement de l'authenticité d'une œuvre en attestant provenance.

Confiance et provenance

Établir la provenance d'une œuvre d'art consiste à fournir son historique et ainsi à en authentifier l'originalité, et à établir sa propriété et sa légalité. L'opération vise à confirmer qu'il ne s'agit pas d'une contrefaçon, ni d'une œuvre volée, pillée ou exportée illégalement.

La qualité de la provenance d'une œuvre d'art peut faire une différence considérable sur sa valeur artistique et donc économique. Cette qualité se juge sur le degré de certitude de l'origine, le statut des anciens propriétaires et la force de la documentation [1]. Cette force provient d'une information vérifiée, dont l'intégrité et la pertinence ne doivent pas pouvoir être remises en cause.

Or, l'essentiel des transactions, des échanges d'œuvres d'art, se fait encore sur papier – un support fragile qui peut être facilement perdu, falsifié ou volé (cela d'autant plus que la pratique n'impose pas de standards ou de normes de chiffrement, d'une part, et de conservation, d'autre part). Parmi ces documents, citons le certificat d'authenticité, pour lequel il n'existe aucune réglementation officielle, tout comme les services et supports de référencement tels les catalogues raisonnés, dont la rigueur méthodologique et l'objectivité sont souvent remises en cause [2].

(1) Wikipedia, https://fr.wikipedia.org/wiki/Provenance
(2) Voir le conflit entre la Mayor Gallery et la société LLC Agnès Martin.

Du reste, la mutation digitale du marché de l'art met en lumière les imperfections (pour ne pas dire les failles) d'un système rendant laborieux et parfois discutable l'établissement d'une provenance fiable des œuvres. La transition numérique en cours ajoute paradoxalement un nouveau niveau de complexité : un grand nombre d'acteurs migrent et opèrent désormais *via* des systèmes d'information (SI) gérés selon une politique propre à chaque organisation et reposant sur des architectures centralisées.

Hormis les risques liés à la sécurité numérique (vol, corruption et manipulation de données), les informations elles-mêmes sont disparates et hétérogènes.

Cette situation crée de fait des opportunités pour la délinquance. Le malfaiteur doit tromper son interlocuteur sur l'œuvre physique elle-même, mais aussi sur son « pedigree » (on parle d'ailleurs de « piège de la provenance »).

Dans un ouvrage [3] qu'il a consacré à cette question, Noah Charney raconte les parcours étonnants des plus célèbres faussaires de l'Histoire :

« La plupart des œuvres d'art sont authentifiées en fonction de leur provenance et des documents qui retracent leur histoire. Les faussaires parviennent à créer un « piège de la provenance ». Bien sûr, le faux doit être assez bon techniquement pour convaincre les experts. Mais la plupart des faux ne sont pas si bons, en dehors du contexte.

Des faussaires qui ne sont pas particulièrement doués peuvent tromper le monde de l'art s'ils réussissent à créer des « pièges de la provenance » suffisamment bons.

C'était le cas de deux célèbres faussaires, John Myatt et John Drewe, qui fabriquaient à la fois l'œuvre et les documents censés attester de son authenticité.

John Myatt ne copiait pas, mais [il] adoptait le style d'artistes célèbres. John Drewe, de son côté, produisait de faux documents et s'introduisait dans les archives pour les y implanter. Lorsqu'un expert voulait se renseigner sur l'œuvre, il se rendait aux archives et, là, miraculeusement, il trouvait une lettre (ou tout autre document) à laquelle personne n'avait fait référence auparavant.

Aujourd'hui, les « héritiers » de John Drewe s'introduisent dans les systèmes d'information, dans les bases de données ! »

En résumé : La fragilité de la documentation, l'absence d'homogénéité dans les pratiques, l'éclatement du marché de l'art, la multiplication des acteurs (opérant de façon isolée) et des systèmes d'information centralisés, leur non-coordination… : l'ensemble de ces éléments rend extrêmement compliqué l'établissement d'une provenance sans faille.

C'est à la lumière de ce constat que la technologie des registres distribués (DLT [4]) ou *Blockchain* apparaît comme une solution idéale pour répondre de manière efficace aux problématiques du marché de l'art dans un contexte multi-agents et multicanal où la traçabilité est un véritable enjeu.

Blockchain : la puissance d'une architecture distribuée et des algorithmes au service de la confiance

La *blockchain* est une innovation technologique ayant le potentiel de modifier radicalement la façon dont nous effectuons les transactions et les rendons traçables.

Il existe quantité de services de certification (tels les coffres-forts numériques), mais ces technologies, dont la gestion et la maintenance reposent sur des architectures centralisées, placent encore l'humain au centre du dispositif, là où la *blockchain* place les algorithmes.

Pour mémoire, la *blockchain* s'est réellement déployée à la fin de 2008, à un moment où s'est effondrée la confiance placée dans les institutions et les organisations humaines supervisant les échanges commerciaux et financiers *via* des systèmes d'information centralisés.

(3) The Art of Forgery, *Noah Charney, Phaidon.*
(4) Distributed Ledger Technology.

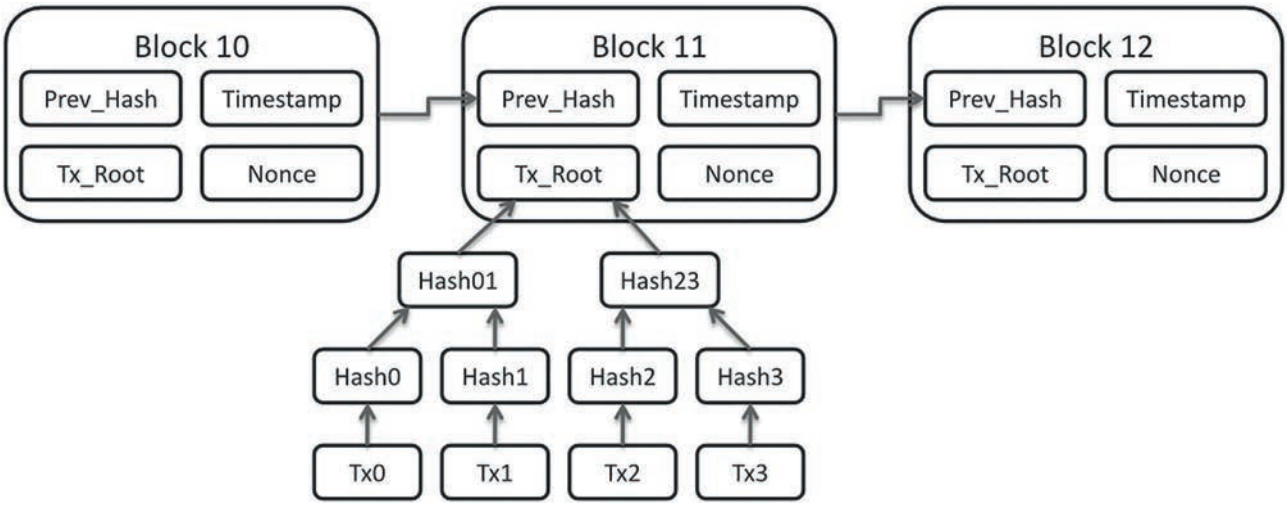


Figure 2 : Schéma du fonctionnement d'une *blockchain*.
Crédit image : Wikimedia Commons.

L'approche de Satoshi Nakamoto, pseudonyme derrière lequel se cache le « Père » de la *blockchain* bitcoin (il existe plusieurs *blockchains* et de types différents), part du postulat suivant : on ne peut faire confiance à l'humain, car il commet des erreurs et il a naturellement tendance à poursuivre ses propres intérêts, avec pour corollaire des tentatives de manipulation, de façon coordonnée ou isolée, afin de tirer parti des transactions à son seul bénéfice.

Une des définitions communément admises de la *blockchain* est la suivante : registre totalement distribué contenant toutes les transactions de façon sécurisée et immuable, dont la gestion et le fonctionnement reposent sur des technologies de chiffrement combinées à un mécanisme de consensus algorithmique, le tout étant réparti sur un réseau pair-à-pair.

Pour faire simple, il faut se représenter une base de données distribuée qui permet de rendre infalsifiable l'historique des transactions, l'ensemble des utilisateurs en possédant une copie et la sécurité étant garantie par l'ensemble des nœuds du réseau (que l'on appelle des « mineurs »), lesquels effectuent les contrôles et vérifications nécessaires sous la forme de résolution d'un problème mathématique que l'on appelle, dans le cas du bitcoin, le *Proof of Work* (preuve de travail).

Cette base de données est ainsi protégée contre toute tentative de manipulation ou de corruption.

Sachant que chaque acteur possède une identité numérique unique vérifiable grâce à la cryptographie asymétrique (c'est-à-dire la combinaison clé privée/clé publique permettant l'identification et l'authentification), un *hash* sera généré qui représentera l'ensemble des éléments d'une opération quelle qu'elle soit.

Cette fonction de hachage est une technique de chiffrement dite « lettre à lettre », elle est irréversible.

Il s'agit d'un chiffrage « lettre à lettre » en ce sens que, si l'on change ne serait-ce qu'un *bit* du message d'entrée (*input*), l'empreinte en sortie (*output*) sera différente.

Exemple : si vous changez une virgule, un espace à un message, la chaîne de caractères correspondant au *hash* sera radicalement différente.

Cette technique est utilisée dans les échanges *peer-to-peer* afin de vérifier que le fichier de destination correspond en tous points au fichier d'origine et qu'il n'y a eu aucune modification, altération ou manipulation.

Cette fonction est irréversible, car on ne peut, à partir du *hash,* reconstituer ou retrouver les informations d'origine.

Cette empreinte pouvant représenter tous les éléments d'une transaction est insérée dans un fichier rassemblant la liste des transactions dites « en attente », ce fichier formant un bloc. Ce bloc sera ensuite validé par les nœuds du réseau – les mineurs – qui, ensemble, contrôleront et conviendront de la validité des transactions *via* un processus de consensus algorithmique : le *Proof Of Work* pour bitcoin, le *Proof Of Stake* pour List ou le *Proof Of Authority* pour Hyperledger.

Prenons le cas du *Proof Of Work* : il s'agit de la résolution d'un problème mathématique destiné à trouver un identifiant pour chaque bloc de transactions à partir des identifiants des blocs précédents (les *hash* Prev_Hash-1 + Prev_Hash-2 + Prev_Hash-n) auxquels s'ajoutent des conditions particulières, telles la recherche d'un nombre, le *nonce*, qui va impacter le résultat du hashage.

Le niveau de difficulté de ce problème est automatiquement ajusté en fonction de la taille du réseau pair-à-pair et de la puissance de calcul, de manière à ce que la résolution ne puisse survenir que toutes les 10 minutes. Un bloc ne peut donc être validé que toutes les 10 minutes.

Une fois le bloc validé, tous les nœuds se synchronisent dessus. Il est alors répliqué sur l'ensemble du réseau pair-à-pair, c'est pour cela que l'on parle de base de données distribuée.

L'ensemble forme donc une chaîne de blocs et en modifier un seul implique que l'on recalcule tous les identifiants de chacun des blocs précédents avant qu'un nouveau soit validé (toutes les 10 minutes).

De fait, la fraude est directement conditionnée à une puissance de calcul qui aujourd'hui n'est pas atteignable en l'état de l'art de la technologie.

Et ce n'est là qu'un aperçu, car sont apparues des *blockchains* dites programmables, comme Ethereum, qui augmentent significativement les possibilités déjà nombreuses de la *blockchain* classique (on parle à leur propos de *smart contracts* : tout en conservant les bénéfices d'une *blockchain*, il est possible de « coder » les termes d'un contrat de manière à ce qu'il s'exécute de lui-même).

Exemple : lors d'une transaction, le certificat d'authenticité pourrait être automatiquement transféré au nouveau propriétaire de l'œuvre, et les droits afférents (droit de propriété, droit de suite, etc.) pourraient être opposables et produire leurs effets eux aussi de façon automatisée.

La *blockchain* est un système d'une résilience et d'une sécurité inégalées, idéal pour protéger les échanges d'actifs matériels et les rendre traçables et auditables, cela d'autant plus que les transactions sont désormais non répudiables. On parle ainsi d'un « Internet de la valeur » !

Appliqué au marché de l'art, il est désormais possible de construire et de garantir une certification et une provenance infalsifiables des œuvres d'art et de réduire les risques de fraude !

Usages et bénéfices pour le marché de l'art

Comme nous venons de le voir, la *blockchain* permettrait d'enregistrer et de certifier tout le parcours d'une œuvre d'art (création, vente, exposition, prêt, legs, restauration...) pour en garantir la provenance fiable et non répudiable, tout en assurant la gestion des interactions entre les parties concernées.

Dès lors, l'authenticité, l'historicité ou encore la valeur d'une œuvre deviennent des informations vérifiées, im-

muables, circulant en toute sécurité entre les acteurs sur toute la chaîne de valeur.

Au-delà de la traçabilité du parcours d'une œuvre, la *blockchain* pourrait bien constituer un nouveau socle technologique pour la propriété intellectuelle et les droits d'auteur.

L'artiste serait assuré d'être la seule personne au monde à pouvoir prouver de façon incontestable la paternité d'une œuvre, les collectionneurs, leur droit de propriété, les galeristes, leur mandat de représentation et certains droits d'exploitation.

Prenons, pour illustrer, deux affaires qui ont marqué le marché de l'art.

L'affaire Peter Doig

L'un des artistes contemporains les plus cotés a dû batailler devant les tribunaux afin de prouver qu'il n'était pas l'auteur d'une peinture, contrairement aux affirmations d'un collectionneur, Robert Fletcher, qui l'accusait de renier une toile qu'il aurait peinte en 1976. Ce dernier souhaitait la vendre aux enchères chez Sotheby's pour plusieurs millions (préjudice : 3 ans de procédure et de frais judiciaires, ainsi que l'anéantissement de la valeur de la peinture).

D.R.

Figure 3 : Peter Doig (né le 12 avril 1959, à Edimbourg).

Conflit entre la Mayor Gallery (Londres) et la société LLC Agnès Martin

Alors qu'une rétrospective de l'artiste Agnès Martin fut présentée à l'automne 2016 au Musée Guggenheim, la galerie d'art londonienne Mayor Gallery a intenté une action en justice contre le Comité d'authentification de la fondation LLC Agnès Martin, qui a refusé d'authentifier 13 œuvres de ses clients lors de la constitution du catalogue raisonné de l'artiste en 2014. En ne reconnaissant pas ces tableaux, la fondation les a privés *de facto* de toute valeur – les clients n'ont d'ailleurs pas tardé à demander leur remboursement (préjudice : 7,2 millions de dollars).

Avec la *blockchain*, ces situations auraient pu être évitées !

Plus globalement, il est possible d'implémenter la gestion et le respect des différents droits résultant de la propriété littéraire et artistique. Outre le droit d'auteur et de propriété, on peut parfaitement envisager le suivi et le déclenchement automatisé du droit de suite, le respect du droit de divulgation, etc.

Il est également possible de développer une infrastructure qui soit de nature à faciliter, simplifier et sécuriser les interactions entre les acteurs opérant sur ce marché. Par exemple, un artiste ou une galerie qui mettrait en vente des œuvres sur une plateforme en ligne et qui, dans le même temps, mettrait à disposition certaines de ces œuvres pour une exposition.

Avec la *blockchain*, la gestion de situations mobilisant plusieurs acteurs sur une même œuvre devient moins complexe, surtout lorsqu'elle fait l'objet de plusieurs opérations autour desquelles s'articulent plusieurs droits et obligations, dont certaines obligations indues : assurances, transport, respect des formalités de douane, etc.

En termes assurantiels, cela permettrait de réduire les risques et de définir plus finement le périmètre des responsabilités. De la même manière, il serait possible de créer de nouvelles polices d'assurances spécifiques pour les besoins d'opérations ponctuelles (prêt, location d'œuvres, *leasing*, etc.) en utilisant pour ce faire des *smart contracts*.

Et ce n'est qu'un début, avec le *machine learning* et le *data mining*, le marché de l'art pourrait bénéficier de nouveaux outils basés sur l'exploitation des données dans le cadre d'une stratégie *Big data* reposant sur une *blockchain* : les perspectives sont immenses.

Aux professionnels de saisir l'opportunité de réinventer les usages tout en capitalisant sur les bonnes pratiques (d'autant qu'un renouvellement générationnel est en cours).

Le marché de l'art est une chrysalide de laquelle peut sortir le meilleur comme le pire. Il ne tient qu'aux acteurs de ce marché d'en décider !

La chaîne du livre et les chaînes de blocs

Par Arnaud ROBERT
Directeur juridique du Groupe Hachette Livre

Hormis pour quelques experts et au sein de quelques expérimentations, la *blockchain* en est encore au stade des promesses. Celles d'usages nouveaux rendus possibles par les qualités majeures qu'on lui prête : celles d'être ouverte mais infalsifiable, d'être fiable même en l'absence de tiers de confiance.
Le monde du livre pourrait y trouver de considérables gains d'efficacité dans ses activités digitales si elle tenait ses promesses de registre inviolable, de médium sécurisé de transfert de fichiers, voire de machine automatique à autoriser, contrôler et percevoir des redevances.
Néanmoins, pour qu'elle constitue l'outil révolutionnaire que l'on annonce, il faudra qu'elle tienne sa promesse la plus ambitieuse, celle d'être un outil de relation d'égal à égal, de pair à pair, au service de tous, et non le jouet de nouveaux intermédiaires monopolistiques.

À l'heure où nous écrivons, le monde du livre et celui de la *blockchain* se sont-ils déjà rencontrés ?

Assurément. À ce stade, cependant, leur rencontre relève d'un paradigme bien connu, qui n'a rien de révolutionnaire ni de disruptif. C'est simplement que le meilleur moyen d'aborder cette nouvelle technologie est sans conteste la lecture d'un bon ouvrage à son sujet. Citons, par exemple, *La Blockchain décryptée*, publié en mai 2016 par l'Observatoire Netexplo, ou *La Révolution Blockchain* de Philippe Rodriguez, publié en mars 2017 chez Dunod.

Pour l'heure, on trouve donc bien la *blockchain* dans les livres. En revanche, la « chaîne du livre », première industrie culturelle de France, est loin d'avoir mêlé, ou même d'avoir songé à mêler ses maillons à ceux de la chaîne de blocs.

C'est que cette technologie, immature et très complexe (pour reprendre les mots de Philippe Rodriguez), s'offre pour l'instant, pour qui n'appartient pas au monde des mathématiciens, des informaticiens ou des cryptographes, plus par les promesses variées à plus ou moins long terme qu'elle contient ou revendique, que par une appréhension très précise de son fonctionnement, éminemment technique, ou de ses mises en œuvre opérationnelles, pour l'heure encore confidentielles (le bitcoin mis à part).

C'est donc à un à exercice purement prospectif que nous conduirons dans ce court article ; celui consistant à confronter les promesses de la *blockchain* (dont nous sommes dans l'impossibilité de valider la robustesse) aux réalités de l'industrie du livre, qui, bien souvent, rejoignent celles des industries culturelles de manière générale.

Le premier temps de l'exercice consistera à identifier les usages que l'avènement de la *blockchain* permettrait ou induirait dans le domaine du livre pour tenter de discerner ensuite en quoi et pour qui ces usages seraient promesse d'opportunités ou, au contraire, de menaces.

La chaîne du livre et les usages annoncés de la *blockchain*

La définition purement technique de la *blockchain*, celle qui s'appuie sur ses modalités informatiques et cryptographiques et sur son protocole fondateur quasi mythique de 2008, ne s'offre qu'aux plus experts.

Très rapidement, on doit donc quitter la technique pour définir la *blockchain* en usant de mots qui ont un sens dans le monde commun. Le concept est ainsi décomposé par le professeur Delahaye, de l'Université Lille 1 : registre – partagé – infalsifiable – indestructible – ouvert – composé de blocs successivement validés, datés et conservés par ordre chronologique.

C'est entendu, mais encore : à quoi cela peut-il bien servir ?

C'est ainsi que fonctionne le bitcoin !, nous rétorque-t-on. Oui, le meilleur (le seul ?) exemple un peu tangible de *blockchain* appliquée, c'est le bitcoin, une monnaie cryptographique qui fonctionne toute seule, sans tiers étatique émetteur. Une monnaie ? Voilà qui est concret ! Mais une monnaie… virtuelle ? Ah !…

Mais si : A veut donner un bitcoin à B. Par la magie de la *blockchain*, un acteur calculateur va décrypter les compo-

sants de la transaction pour la valider et une communauté d'autres calculateurs va attester de cette validité. L'opération, une fois validée, aura une existence dans la chaîne, scellée au sein d'un bloc, consultable par tout un chacun.

C'est un générateur de confiance. Confiance dans la propriété originelle de A, confiance dans l'existence de la transaction de A vers B et, enfin, confiance dans la qualité de nouveau propriétaire de B. Et cette confiance n'a pas été validée auprès d'un tiers unique disposant du monopole de la certification, mais par le biais d'un « consensus décentralisé ». La *blockchain*, ce serait la « confiance distribuée », pour reprendre le titre de l'ouvrage paru en juin 2016 sous l'égide de Fondapol (un *think tank*) (http://www.fondapol.org/wp-content/uploads/2016/06/083-SOUDOPLATOF-2016-05-26-webDEF.pdf)

Malgré cet exemple, le brouillard conceptuel n'est pas totalement dissipé. Assez rapidement, donc, les débats à propos de la *blockchain* s'orientent vers les usages dont cette technologie s'annonce porteuse.

Dans le domaine des industries culturelles, et donc, potentiellement, du livre, ces usages sont classiquement envisagés autour de trois grands axes :

1) un registre des droits d'auteur,
2) le médium permettant la circulation des livres numériques,
3) une gestion automatisée personnalisée des droits d'auteur.

La *blockchain*, un registre des droits d'auteur

Une autre appellation de la *blockchain* est celle de « *distributed ledger technology* », la « technologie du registre distribué ». En d'autres termes, un registre ouvert à la consultation et à son enrichissement, mais infalsifiable du fait de sa validation par consensus décentralisé.

La *blockchain* comme registre, c'est ce qui est annoncé pour munir d'un cadastre le Ghana ou la Géorgie. La *blockchain* atteste de la propriété foncière dans un registre ouvert, facilement accessible et consultable, et pourtant infalsifiable. Ici, le registre fait preuve : preuve d'un droit de propriété, d'une date de transfert, d'une chaîne de droits.

Une autre application est avancée pour la *blockchain*-registre : la traçabilité et la certification. La *start-up* Everledger s'emploie à construire un registre numérique destiné à recenser les transactions diamantaires de manière à lutter efficacement contre le vol et la fraude. Pour en permettre l'enregistrement, chaque diamant se voit attribuer un numéro de série. Ce numéro de série est micro-gravé sur la pierre précieuse et est enregistré en parallèle dans la *blockchain*.

Preuve d'origine, de date, de propriété, la *blockchain* comme registre est susceptible d'intéresser le monde de la création, dont les actifs sont par essence immatériels (ils le sont même doublement maintenant que leurs supports eux-mêmes sont numériques : fichiers MP3 ou ePub…)

L'industrie musicale réfléchirait déjà à une grande base de données de droits d'auteur fondée sur la *blockchain*.

Un titre musical contient au moins deux *copyrights* : l'un pour le son, l'autre pour le texte et la composition. Comme l'explique le site de Blockchain France, « la preuve d'existence et d'appartenance de ces deux *copyrights* pourrait être stockée sur la *blockchain*, […] permettant d'enregistrer de façon incorruptible la propriété de chaque titre et les *copyrights* correspondants ».

Dans le monde du livre, la chaîne des droits est moins éclatée que dans celui de la musique, et les éditeurs perçoivent généralement tous les revenus d'exploitation des livres qu'ils ont publiés, à charge pour eux d'en assurer le partage entre les différents contributeurs à un livre : auteur, traducteur, illustrateur, photographe…

La multitude de droits protégeant une œuvre donnée est donc moins problématique dans l'univers de l'écrit que dans celui de la musique.

Néanmoins, on peut imaginer le réel intérêt que présenterait un registre qu'une multitude d'acteurs pourrait nourrir et qui resterait infalsifiable : un registre centralisé des auteurs français, à l'instar de ce que la Société des Gens de Lettres entreprend *via* son fichier Balzac, ou un registre des œuvres elles-mêmes.

Ce registre pourrait être alimenté par tous ceux qui ont à connaître de la vie d'une œuvre ou d'un auteur, sans risque de falsification : les éditeurs à chaque nouvelle œuvre ou réédition, la Bibliothèque Nationale de France lors du dépôt légal de toute nouvelle parution, les notaires lors du décès de l'auteur, l'auteur lui-même lors d'un changement d'adresse...

Car les récents projets de numérisation des fonds anciens ont tous révélé les mêmes limites : comment retrouver les auteurs d'œuvres éditées depuis plusieurs décennies, ou *a fortiori* leurs héritiers ? Pour les œuvres, comment combler les lacunes de leurs métadonnées originelles ? Devant ce manque de répertoire, les tenants du tout-gratuit ou de l'accès universel à la connaissance ont parfois beau jeu d'expliquer que, face à l'incapacité d'identifier les titulaires de droits, il faudrait autoriser d'immenses exceptions au droit d'auteur.

La *blockchain*, ce medium permettant la circulation des livres numériques

Les œuvres sont depuis plusieurs années publiées au format numérique en même temps qu'elles sont imprimées. Leurs versions numériques sont vendues sur de grandes plateformes d'e-books, comme elles le sont sur les sites des libraires de quartier. Leur vente fonctionne par analogie à celle du monde physique : en contrepartie du paiement en ligne, le client télécharge un fichier qui, désormais, lui appartient.

Mais l'analogie n'est pas parfaite : le livre numérique ne peut être prêté ou revendu, car, dans le monde numérique, l'expression « transfert de fichier » est un pur abus de langage : il s'agit à chaque fois de la reproduction d'un fichier, dont on envoie la copie à un tiers, tandis que l'on conserve le fichier initial. Il s'agit, donc, à chaque fois, d'un acte de piratage ! Des mesures techniques de protection empêchent donc les actes de reproduction autres

que ceux qui permettent à l'acquéreur d'une œuvre de la lire sur des moniteurs de différentes natures.

Avec la *blockchain* telle qu'elle est promise, l'analogie semble pouvoir être approfondie. Dans la *blockchain*-type du bitcoin, il y a bien cette opération de dessaisissement que l'on trouve dans le monde physique : le bitcoin que A transfère à B quitte bien le patrimoine de A pour intégrer celui de B. L'opération est irréversible et scellée dans la chaîne de blocs. On peut dire que ce bitcoin donné a une identité propre. Si, au lieu du bitcoin, on transférait un livre numérique, on pourrait considérer que c'est bien le « même » livre qui circule, sans opération de reproduction contrefaisante.

En extrapolant au-delà du monde du livre, on pourrait dire que la *blockchain* ouvre la voie à la naissance de réels « biens » numériques, revêtus d'une unicité.

Le lieu n'est pas ici d'explorer les perspectives ouvertes par cette « naissance ».

Pour l'éditeur, disons seulement qu'elle emporte des promesses autant que des menaces : un livre numérique voyageant dans la *blockchain* sur un support individuellement identifié permettrait à son propriétaire une « expérience utilisateur » proche de celle du livre physique (accès plus pérenne et plus « interopérable », quel que soit l'environnement de lecture ou de conservation) et faciliterait la protection contre la contrefaçon, grâce à la traçabilité induite par la chaîne de blocs ; son rapprochement avec le livre physique ouvrirait à l'inverse la porte à de dangereux concepts du monde physique dans l'économie du monde numérique : épuisement des droits après la première vente du fichier, revente de livres d'occasion…

La gestion automatisée et personnalisée des droits d'auteur

Au sommet du panthéon de la *blockchain* bruisse la mécanique quasi magique des *smart contracts*. Décrits comme des programmes autonomes qui exécutent automatiquement des conditions définies à l'avance, ils serviraient de supports à des contrats auto-exécutables.

En d'autres termes, couplé à un dispositif de paiement par crypto-monnaie, le fichier d'un livre numérique pourrait porter en lui à la fois :

- ses conditions d'usage (lecture individuelle, prêt en bibliothèque, reproduction dans le cadre d'un enseignement, adaptation audio…) ;
- le paiement immédiat, au moment de son usage, des redevances dues (en fonction du type d'usage qui en est fait) ;
- une redirection instantanée vers les différents ayants droit (auteurs, illustrateurs, éditeurs, société de gestion collective…) de la part des redevances leur revenant.

Ces *smart contracts* permettraient ainsi d'individualiser, de personnaliser, d'optimiser les conditions et les tarifs d'usage de chaque livre numérique, et de raccourcir et donc d'accélérer les délais de perception des droits d'auteur.

La chaîne du livre et les ruptures prédites par la *blockchain*

Il n'est pas une conférence ou un article qui ne justifient leur existence par le caractère profondément disruptif de la technologie *blockchain*.

Nous l'avons dit, il nous semble qu'à ce stade, la *blockchain* se définit plus par les promesses qu'elle porte que par les réalisations concrètes qu'elle fonde.

Ces promesses, pour l'instant, se résument dans une sorte de mantra : la *blockchain* serait en capacité de donner à chaque agent (entreprise, client, usager, citoyen…) intervenant sur le *Web* l'autonomie et le contrôle qui lui manquent depuis la naissance d'Internet, le paradis jamais atteint de la relation pair-à-pair.

De ce mantra, s'il devait exprimer au bout du compte une réalité, découleraient des opportunités et des risques pour la chaîne du livre.

Les opportunités de la *blockchain* pour le livre

Technologie permettant l'identification et le transfert d'un livre numérique comme s'il s'agissait d'un livre physique ; registre infalsifiable, public, ne faisant pas appel à un tiers centralisateur ; technologie portant en elle la capacité de gérer des contrats auto-exécutables… : par toutes ces qualités, la *blockchain* serait en capacité de donner à l'auteur ou à l'éditeur de livres numériques un contrôle accru sur ses créations ou ses activités grâce à :

- une gestion directe, sans intermédiaire, de la commercialisation (plateforme de distribution) ou une gestion des droits (société de gestion collective), avec des lecteurs mieux connus dans leurs caractéristiques et leurs pratiques ;
- une gestion granulaire des droits attachés à un livre numérique donné, par type d'usage et par client ;
- un raccourcissement des circuits de paiement ;
- une traçabilité parfaite des biens numériques mis en circulation sur les réseaux, facilitant ainsi la prévention des copies illégales.

Les risques de la *blockchain* pour le livre

Le discours sur la *blockchain* prend pour acquise la robustesse du modèle technique sur lequel elle fonde sa révolution. Si ce postulat devait se révéler exagérément optimiste, les risques seraient les suivants :

- infalsifiable, la mécanique de la *blockchain* repose pourtant sur un consensus, lui-même fondé sur une règle de majorité en termes de puissance de calcul : s'il faut 51 % d'une puissance de calcul donnée pour valider une transaction, les mêmes 51 % permettent *a priori* de la défaire ;
- dupliquée, la *blockchain* reproduit et dissémine les données les plus variées sur tous les serveurs du globe, rendant difficile l'appréhension d'un responsable en cas d'acte illégal perpétré par son intermédiaire ;
- décentralisée, la promesse majeure de la *blockchain* est celle de la désintermédiation ultime. On pourrait y voir

un danger pour un acteur comme l'éditeur, si l'on pense que celui-ci, intermédiaire entre l'auteur et les lecteurs, pourrait se voir effacer de la chaîne avec les autres intermédiaires, les distributeurs et les libraires, pour laisser la place à un auteur gestionnaire direct de l'exploitation de ses livres, distribuant et facturant directement ses œuvres *via* la *blockchain*. Ce serait probablement oublier que l'éditeur agit d'abord en tant que sélectionneur, puis comme collaborateur et, enfin, comme promoteur des livres pour les faire vivre au sein de l'offre immense qui se présente au lecteur.

En réalité, la désintermédiation nous paraît receler un danger bien plus grand, celui d'être une fausse promesse masquant l'émergence de nouvelles superpuissances économiques en capacité d'imposer leurs exigences à tous les opérateurs qui voudront emprunter les voies chaînées qu'ils contrôleront.

Car si la *blockchain* fera (peut-être) disparaître certains intermédiaires, il s'en créera d'autres : les opérateurs des « nœuds », rouages essentiels et rémunérés de la chaîne ; les plateformes d'échanges de monnaies cryptographiques ; les détenteurs de l'information certifiée, qui seule permettra de déclencher les *smart contracts* ; et enfin, et surtout, celui qui, le premier, saura créer la technologie intercalaire entre la machinerie cryptée de la *blockchain* et l'usager commun (à la manière dont le *Web* est venu s'intercaler entre les utilisateurs et le réseau Internet, permettant son usage le plus large, mais au prix du passage par des opérateurs de navigation devenus quasi monopolistiques à l'échelle mondiale).

La *blockchain* au service de l'action publique

Par Malo CARTON
Ingénieur des mines, Agence des participations de l'État (APE)
et Pierre JÉRÉMIE
Ingénieur des mines, chef du service de prévention des risques et des nuisances, direction régionale et interdépartementale de l'environnement et de l'énergie (DRIEE) d'Île-de-France

La technologie *blockchain* offre la possibilité de construire des registres décentralisés et de partager la confiance entre opérateurs dans la validité de ces registres. La décentralisation des bases de données sous-jacentes à une *blockchain* est consubstantielle à cette technologie. Dans le cas de l'action publique, une telle décentralisation constitue un changement de paradigme pour l'organisation habituelle de données publiques jusque-là stockées par un ou plusieurs opérateurs publics étroitement surveillés. Nous présenterons ici deux champs d'action publique pour lesquels la mise en œuvre de solutions utilisant cette technologie est actuellement à l'étude : la mise en place d'une nouvelle chaîne de titres pour assurer une circulation des titres financiers plus fluide, mais aussi plus aisément contrôlable, et les possibilités offertes par la *blockchain* pour l'enregistrement des droits et des servitudes sur les sols au service d'une meilleure information des acquéreurs.

Introduction

Alors qu'à l'origine, par le biais de la communauté d'utilisateurs du protocole bitcoin, la technologie *blockchain* s'est construite par opposition au modèle centralisé standard prévalant dans l'action gouvernementale, selon une conception « libertarienne » des rapports économiques et sociaux, les promesses de la technologie ont amené les gouvernements de plusieurs pays de l'OCDE (dont la France), à considérer avec attention les applications potentielles d'une telle technologie. Nous nous proposons, dans cet article, de présenter quelques caractéristiques de la *blockchain* qui peuvent justifier l'intérêt qu'a suscité cette technologie dans le cadre de l'action publique. Deux exemples seront plus amplement détaillés, l'un étant tiré de l'actualité législative récente, et l'autre plus exploratoire afin de mettre en avant quelques applications types qui sont attendues de cette technologie dans le cadre de l'action publique.

Les principales caractéristiques de la *blockchain* présentant un intérêt pour l'action publique

Une *blockchain* est avant tout une méthode d'implémentation d'un registre distribué (c'est-à-dire réparti entre les différents nœuds d'un réseau) et protégé contre des modifications des données enregistrées, y compris de la part de ceux qui la mettent en œuvre.

Schématiquement, deux types d'opérateur sont présents sur une *blockchain* :

- d'une part, des utilisateurs qui souhaitent voir stockées des informations et/ou consulter des informations qui le sont déjà ;
- d'autre part, des « mineurs » : ce sont des utilisateurs qui mettent à la disposition du réseau, souvent contre une rémunération déterminée dans le protocole, leurs capacités de calcul dans le cadre d'une preuve de calcul (*proof of work*) pour assurer la validation des informations et la gestion décentralisée du registre.

Au-delà des différentes technologies envisageables pour mettre en œuvre une *blockchain*, il convient tout d'abord d'examiner (dans le cadre de cet article) les propriétés fondamentales des *blockchains* qui peuvent s'avérer intéressantes pour l'action publique :

- leur caractère distribué permet de répartir la charge de la mise en œuvre de ces registres entre un grand nombre d'utilisateurs, y compris hors État (collectivités, opérateurs agréés, etc.) ;
- leur construction rend les *blockchains* résilientes à des attaques : en pratique, les données stockées sont gravées dans le marbre, définitivement, et ne peuvent être altérées (y compris par les opérateurs du registre), une fois qu'elles ont été validées [1] ;

(1) Cela tant que des évolutions techniques ne permettent pas de casser en un temps relativement court les chiffrements employés ou la « preuve de travail » de la blockchain.

- elles permettent de construire structurellement un consensus sur la validité des données enregistrées et sur leur chronologie ;
- n'importe quel nœud d'une *blockchain* peut aisément vérifier si une donnée figure ou non dans la base.

La décentralisation des bases de données sous-jacentes à une *blockchain* est consubstantielle à cette technologie. Dans le cas de l'action publique, une telle décentralisation peut conduire à modifier en profondeur l'organisation habituelle de données publiques qui jusqu'ici étaient stockées par un ou plusieurs opérateurs publics étroitement surveillés. Cette décentralisation va de pair avec la vérification par n'importe quel nœud (c'est-à-dire par n'importe quel utilisateur) des données qui figurent dans la *blockchain*. Suivant les décisions de politique publique souhaitées, on peut imaginer, grâce à cette technologie, d'offrir aux citoyens la possibilité d'accéder à un haut niveau de transparence, tout en leur permettant de participer activement au système, en en représentant des nœuds stockant une partie des données. Cela pose nécessairement la question du champ d'ouverture de ces données : souhaite-t-on par exemple les ouvrir à tous les citoyens, dans un souci de transparence (à l'instar, par exemple, du cadastre, ou des données sur l'état de l'environnement [2]) ?

Par ailleurs, pour conforter la résilience de la *blockchain* (inaltérabilité des données inscrites) procédant du protocole de validation des blocs, et notamment de la force du consensus, la question des mineurs est cruciale, dans le cas d'une *blockchain* destinée à l'action publique. Là encore, on peut imaginer mobiliser une technologie *blockchain* comme moyen permettant de donner du pouvoir aux citoyens, en leur conférant un pouvoir de vérification renforçant d'autant la confiance que peuvent susciter les données concernées.

En raison de ses principales caractéristiques, la *blockchain* apparaît dès lors être un moyen de refonder certains modes de fonctionnement en conférant aux citoyens (ou à un sous-ensemble de citoyens) un pouvoir aujourd'hui réservé ou fortement interfacé par la puissance publique. Dans un contexte de défiance vis-à-vis de certaines institutions de contrôle, les promesses d'une telle technologie plus consensuelle et horizontale peuvent être intéressantes. Plus prosaïquement, on peut aussi considérer que, dans certains cas, la mise en place par l'État d'un tel système pourrait conduire à une organisation plus efficace de systèmes aujourd'hui sujets à des rentes de situation ou à des inefficiences technologiques (voir les exemples des titres financiers, ci-après).

Blockchain et action publique : deux déclinaisons concrètes

De la monnaie électronique à la construction d'une nouvelle chaîne de titres au service du financement de l'économie et d'un meilleur suivi des transactions

Comme évoqué plus haut, la technologie de la *blockchain* permet d'implémenter de manière décentralisée un registre résistant à des attaques, enregistrant des données de manière définitive et partagée, avec un consensus des utilisateurs sur le contenu de ce registre. Un grand nombre de métiers requièrent des registres inaltérables, consensuels et publics. Ils étaient, de ce fait, irréalisables – avant l'irruption du numérique – en l'absence d'une autorité centralisée certifiant l'inaltérabilité et venant apporter sa garantie valant consensus. Ils étaient donc en général confiés soit aux États, soit à des opérateurs privés de grande taille (le plus souvent soumis à un fort contrôle public).

L'exemple d'utilisation de la *blockchain* le plus connu du grand public est le protocole bitcoin, pour lequel le registre implémenté est un registre de transactions d'une monnaie virtuelle grâce auquel la *blockchain* permet de décentraliser la confiance dans la régularité des transactions et la validité de la monnaie présentée (un rôle confié de tout temps, pour les monnaies fiduciaires ou métalliques, à l'État ou à une banque centrale disposant d'un monopole, s'érigeant ainsi en « tiers de confiance » ultime).

Parmi les nombreuses applications attendues de la « chaîne de blocs », l'évolution des modalités de représentation et de circulation des titres financiers suscite l'attention du secteur financier : des financements importants sont d'ores et déjà mobilisés, en France, mais surtout dans les pays anglo-saxons.

Si le droit applicable aux titres financiers – et le fonctionnement des infrastructures et acteurs associés (dépositaire central de titres, teneurs de compte, etc.) – est longtemps resté discret, sinon inconnu, c'est que ce domaine cantonné à un débat d'experts, entre juristes et « titrards » des établissements financiers, était perçu comme moins stratégique que celui de la négociation (la corbeille) ou de l'orchestration des opérations sur le capital.

Toutefois, en l'absence d'une chaîne robuste du titre, le transfert de propriété des titres, contrepartie juridique du règlement d'une transaction financière en espèces, ne peut être garanti. C'est dès lors le fonctionnement des marchés financiers qui est remis en cause dans son fondement même. Tant pour des raisons opérationnelles que pour des raisons de supervision des acteurs, les participants de la chaîne du titre ont été historiquement centralisés, ou au moins organisés en « arbres », chaque nœud représentant un teneur de compte, et le nœud de plus haut niveau représentant le dépositaire central. Pour une transaction donnant lieu à un transfert entre deux participants qui ne sont pas les clients d'un même teneur de compte, l'opération doit être validée par chacun des deux teneurs de compte, qui doivent eux-mêmes en référer au dépositaire central responsable de l'intégrité de l'ensemble des titres en circulation.

Cette logique est fondamentalement antagonique avec la logique du protocole *blockchain*. Les transactions ne sont pas validées par consensus décentralisé entre tous les acteurs de marché, mais par un seul intermédiaire, centralisé

(2) *Convention d'Arhus, directive INSPIRE.*

et fortement régulé (compte tenu du pouvoir exorbitant qui lui a été ainsi conféré). Incidemment, il convient de noter que cette organisation peut rapidement s'avérer problématique du point de vue économique, en raison de la présence d'un acteur en situation de monopole de fait qui peut être tenté de prélever une rente sur les utilisateurs. Historiquement, la solution qui avait été trouvée consistait à faire participer les principaux acteurs financiers au capital du dépositaire central (c'était le cas en France, avec la Sicovam, détenue à l'origine principalement par des banques françaises), ce qui permettait de limiter le risque d'un comportement de rentier de la part du dépositaire.

Dans ce contexte, que peut apporter la chaîne de blocs au fonctionnement de la chaîne du titre ?

Tout d'abord, elle permet d'éviter une structure arborescente, qui ferait reposer l'intégrité de la chaîne sur un seul maillon, le nœud de plus haut niveau, qui devrait être très fortement régulé, ce qui conduirait en retour à un possible comportement de rentier de la part de cet acteur, et ce, au détriment de l'ensemble du système (coûts excessifs, inefficiences, etc.).

Par ailleurs, dans le cas des titres non cotés, la mise en place d'une solution chaîne de blocs représenterait un important saut technologique comparable à la dématérialisation des titres cotés intervenue en France en 1984. Cela serait de nature à favoriser l'écosystème du financement désintermédié, en renforçant la robustesse et la vérifiabilité des transactions portant sur des titres non cotés.

Enfin, en consignant dans un registre décentralisé l'ensemble des transactions sur les titres, et non pas en donnant une image statique des propriétaires des titres à un instant donné, le niveau d'information auquel peuvent avoir accès d'éventuels contrôleurs (administration fiscale, Autorité des marchés financiers) serait substantiellement renforcé, leur permettant à tout instant de disposer d'une vision du portefeuille des acteurs du marché et d'en reconstruire l'historique.

Dans ce contexte, des avancées ont été annoncées par le précédent gouvernement pour promouvoir le développement de cette nouvelle technologie.

Deux annonces successives ont été faites : tout d'abord, l'annonce d'une expérimentation pour l'utilisation d'une chaîne de blocs pour les « minibons » (ordonnance du 28 avril 2016 relative aux bons de caisse), puis l'annonce d'un cadre réglementaire pour l'utilisation d'une chaîne de blocs pour les titres financiers non cotés dans le cadre de la loi relative à la Transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « loi Sapin 2 ».

Les minibons sont des instruments de financement, qui, sans être des titres de créance ou des contrats de prêt, matérialisent une reconnaissance de dette sur une entreprise. Il s'agit d'une remise au goût du jour d'un vieil instrument de financement, le bon de caisse, dans le cadre du financement participatif.

L'ordonnance précitée, prise en application de la loi « Macron », a permis de réformer le cadre réglementaire des bons de caisse afin de créer les minibons. Durant les travaux préparatoires de l'ordonnance, il a été jugé opportun de réserver au niveau législatif la possibilité de mettre en place, par décret pris en Conseil d'État, un mécanisme du type chaîne de blocs pour la représentation et la mise en circulation de ces nouveaux instruments de financement.

Cela a ainsi permis d'inscrire au niveau législatif, dès le début de l'année 2016, la première définition d'une chaîne de blocs en droit français au sein du Code monétaire et financier (et, à la connaissance des auteurs, en droit européen) :

« Art. L. 223-12 – Sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations dans des conditions, notamment de sécurité, définies par décret en Conseil d'État. »

La solution retenue présente l'avantage de l'optionalité, tout en réservant de la place à l'expérimentation de ce nouveau mode de fonctionnement des activités de post-marché, si les circonstances sont réunies.

Cette solution a été possible dans le cadre de cette ordonnance, car, contrairement à l'univers des titres financiers (surtout ceux qui sont cotés), le régime juridique applicable aux bons de caisse était quasiment inexistant et ne procédait d'aucun texte européen. L'espace était donc libre pour mettre en place les premiers jalons d'un cadre nouveau, qu'il conviendra de préciser lors de l'adoption du décret prévu à l'article L. 223-12. Toutes choses égales par ailleurs, on peut rapprocher cette situation de celle du développement des télécommunications mobiles dans les pays en développement : il est parfois plus simple de passer tout de suite au meilleur niveau de l'état de la technique lorsque l'on part d'une « feuille blanche ».

S'agissant de la loi Sapin 2, une habilitation à procéder par voie d'ordonnance a été prévue pour définir un cadre réglementaire en vue de la mise en place d'une solution de type *blockchain* pour des titres non cotés. Une consultation publique est en cours pour déterminer les contours de la régulation qui pourrait ainsi être mise en place. La France sera alors l'un des premiers pays en Europe à se doter d'un tel cadre réglementaire, qui pourra éventuellement être étendu au cadre européen, notamment pour les titres cotés [3].

Dans les deux cas, en partant des avantages du cadre existant et des contraintes juridiques applicables, l'approche suivie à ce jour en France pour l'application de la technologie chaîne de blocs à la chaîne du titre est à la fois graduelle et hybride.

Graduelle, elle l'est pour initier les expérimentations dans des cas d'usages naissants (minibons) ou en complément d'un cadre existant peu satisfaisant (titres non cotés).

(3) http://www.tresor.economie.gouv.fr/16101_consultation-publique-ordonnance-blockchain-applicable-a-certains-titres-financiers

Hybride, elle l'est lorsqu'il s'agit de ne pas basculer l'ensemble du cadre de représentation et de circulation des titres dans la chaîne de blocs, pour chercher, au contraire, à appuyer le développement de la chaîne de blocs, notamment au service de l'enregistrement des transactions, en misant sur la force juridique de la représentation des comptes-titres. La chaîne de blocs peut alors devenir un nouveau mode, davantage décentralisé, d'administration d'un compte-titre centralisé, qui continuerait à avoir force juridique pour ce qui est de la propriété des titres.

Blockchain et livre foncier : vers l'intégration dans le système des titres de propriété à l'attention des acquéreurs d'informations sur les risques et les nuisances

Une autre mission particulièrement régalienne des États est l'implémentation du cadastre, d'une part (au sens de registre public des parcelles existantes par entité administrative), et d'un registre des propriétés foncières, d'autre part, certifiant la propriété de ces parcelles. Ce travail, dont on trouve des traces depuis la plus haute antiquité, remplit plusieurs fonctions : d'une part, apporter la connaissance des assiettes fiscales pour les impôts calculés sur une base foncière, dont la publicité et l'inaltérabilité sont des garanties démocratiques acquises lors de la Révolution française et, d'autre part, apporter la garantie publique aux titres de propriété foncière.

Il est parfaitement envisageable, sur un plan technique, de numériser ces deux documents dans un registre de type *blockchain*, répondant, par construction, aux impératifs de publicité, d'inaltérabilité et de consensus requis. Plus concrètement, les autorités publiques ayant pouvoir sur le cadastre ou assurant la validité légale et la certification des changements de propriété foncière (les notaires, notamment) pourraient être les « mineurs » d'une *blockchain* rendant accessibles à tous les données de tel ou tel propriétaire. La plasticité d'un tel registre permettrait d'ailleurs d'intégrer dans un registre décentralisé unique d'autres types de données, notamment, pour les différentes parcelles, les informations relatives aux prescriptions d'urbanisme applicables et toute information relative à ces parcelles.

Il devient ainsi imaginable de construire un système décentralisé d'enregistrement des mutations foncières dans lequel les transactions immobilières seraient saisies par des officiers ministériels (les notaires, par exemple), ce qui permettrait à l'administration de disposer également, à des fins fiscales, de l'inventaire des propriétés parcellaires, soit l'ensemble des fonctions actuellement remplies par le livre foncier. En pareil cas, outre ces transactions, le registre décentralisé de la chaîne de blocs permettrait également de saisir des « transactions spéciales » qui viendraient simplement « rattacher » aux parcelles les prescriptions applicables ou les données environnementales afférentes, dans une base de données décentralisée. Ainsi, on pourrait imaginer qu'un service chargé de l'urbanisme puisse disposer des droits lui permettant de rattacher à une parcelle les prescriptions prévues dans le plan local d'urbanisme et dans les plans de prévention des risques ou les servitudes d'utilité publique applicables, qu'un service chargé du suivi des pollutions existantes des sols puisse saisir les informations relatives aux secteurs d'information sur les sols issus de la loi ALUR (art. 173) en en assurant une consultation facilitée et une mise à disposition « en une fois » pour d'éventuels acquéreurs. En automatisant la mise à disposition des données environnementales et des règlements d'urbanisme attachés à une parcelle, un tel dispositif permettra non seulement de réaliser des gains importants d'efficience en abolissant les consultations systématiques des services en charge de ces questions lors des mutations foncières, en fluidifiant les transactions immobilières et en facilitant l'identification tant de situations problématiques que les secteurs les mieux appropriés à des projets d'aménagements. La construction du dossier préalable à une acquisition (la liasse, fort épaisse, qu'il convient de parapher devant notaire) ne prendrait plus que le temps d'un clic pour retrouver les informations pertinentes sur le bien considéré.

Le rôle de l'État passerait de celui d'autorité de certification d'un registre centralisé des données à un rôle de garant de l'intégrité du protocole et des moyens de chiffrement mis en œuvre, ce qui suppose un renversement d'optique de première importance pour ces missions très régaliennes. La mise en œuvre de cadastres numériques décentralisés basés sur la chaîne de blocs pourrait cependant trouver une application dans des pays en développement ne disposant pas de registre centralisé et dans lesquels la garantie des droits de propriété représente un enjeu fort pour le développement économique. Une expérimentation en la matière est le projet Bitland, qui vise à déployer un tel dispositif au Ghana [4]. Là encore, comme dans le cas des minibons, il est parfois plus simple d'aller directement à la pointe de la technologie, quand on part d'une feuille blanche.

Conclusion

À l'heure où émerge la chaîne de blocs, celle-ci peut apparaître comme une opportunité de restaurer une horizontalité entre utilisateurs du réseau, en en faisant simultanément des prestataires et des utilisateurs de services tant numériques que réels, dans une approche pair-à-pair : l'action publique a tout à gagner à se saisir de cette possibilité pour assurer le maintien des registres d'opérations ou de propriété au service du contrôle, dans des domaines aussi distincts que le suivi des droits et servitudes foncières ou la maîtrise de la chaîne de titres. Cette évolution permettra non seulement une meilleure fluidité des échanges, mais également un contrôle plus aisé des opérations, conduisant à un fonctionnement efficient des marchés. Cette évolution supposera toutefois une évolution substantielle de la relation contrôleur/contrôlé, en plaçant les contrôlés en capacité d'assurer une partie du contrôle de la correction des saisies dans la chaîne.

(4) http://bitlandglobal.com/

Les infrastructures et les services de l'Internet

Par Stéphane BORTZMEYER
Ingénieur à la direction des systèmes d'information et des opérations de l'Association française pour le nommage Internet en coopération (AFNIC)

De nombreuses applications ont été proposées pour la chaîne de blocs (*blockchain*). Mais on doit constater que, dans beaucoup de cas, la description de « comment » la chaîne de blocs pourrait être utilisée pour cette application est tellement approximative qu'il est impossible d'évaluer si l'utilisation de la chaîne de blocs est, dans ce cas, raisonnable. Or, cette chaîne n'est pas utile pour toutes les applications.
Nous explorerons ici deux applications liées à l'infrastructure de l'Internet : les journaux (au sens de journal de bord) et, surtout, les registres de noms, pour lesquels il y a déjà eu d'innombrables débats sur leur fonctionnement.
Comment un registre de noms peut-il être réalisé sur une chaîne de blocs ? Qu'y gagnerait-on ? Quels seraient les problèmes et les obstacles ?

Depuis que le concept de chaîne de blocs (*blockchain*) est à la mode, d'innombrables articles et présentations en ont exposé des applications possibles, souvent décrites en des termes très vagues (« il sera désormais impossible de mentir sur son diplôme, grâce à la *blockchain* », « les données de santé seront dans la *blockchain* »…). Ce flou fait qu'il est difficile de discuter de ces applications, ou même de voir si la chaîne de blocs est vraiment une solution adaptée à ce problème.

Notre but sera ici, au contraire, de détailler les applications de la chaîne de blocs pour les services de base de l'Internet, ainsi que pour son infrastructure.

Deux types de services « blockchainisables »

Le bon fonctionnement de l'Internet dépend d'un certain nombre de registres. Un registre est un service par lequel on va assurer l'unicité et la bonne gestion de certaines ressources, ainsi que la conservation de données sociales. Par exemple, un nom de domaine doit être unique. Les données rares (comme les adresses IPv4) doivent être sévèrement rationnées. Le nom et l'adresse de l'organisation qui a enregistré un numéro de système autonome – un nombre indispensable au fonctionnement du protocole de routage BGP (*Border Gateway Protocol*) – doivent être enregistrés.

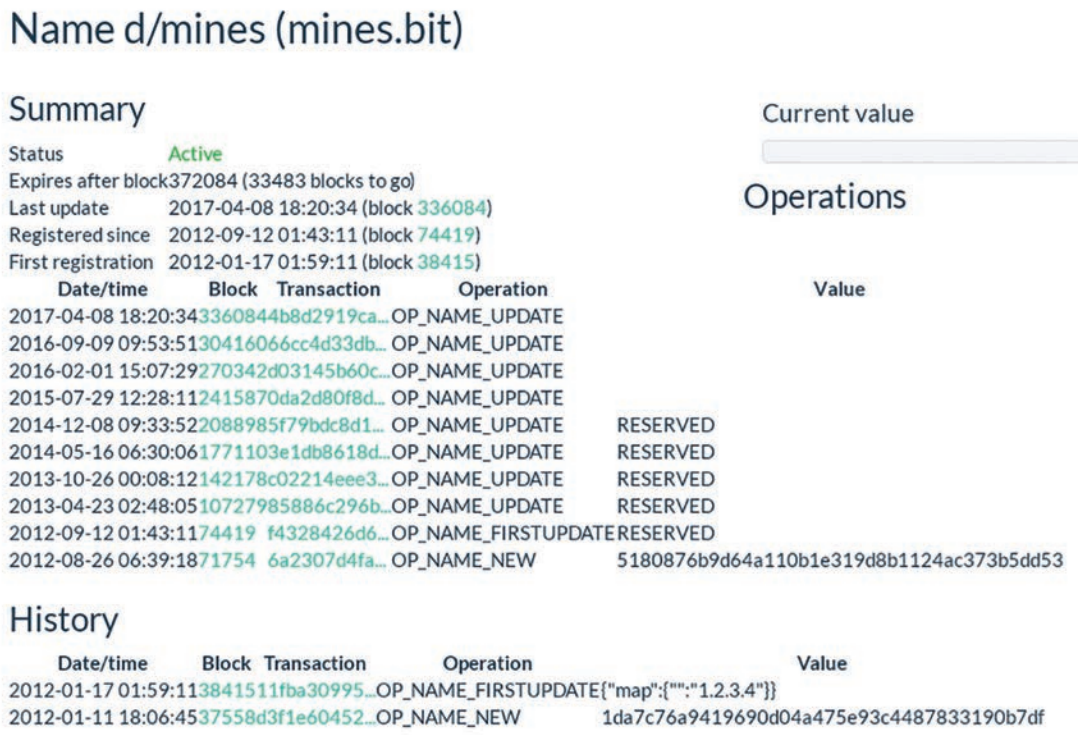
Le terme de « registre » désigne non seulement le service, mais aussi l'organisation qui assure ce service. Avant la chaîne de blocs, la sagesse conventionnelle était en effet que ce service devait être assuré par une organisation unique qui recevait les demandes, jugeait parfois de leur acceptabilité, mettait les enregistrements dans une base de données et, enfin, en assurait la publication.

C'est ainsi que l'AFNIC est le registre du domaine « .fr ». C'est son intervention qui assure qu'il n'y aura qu'un seul paris.fr ou qu'un seul wikipedia.fr, que l'on pourra retrouver le nom et l'adresse du titulaire de ces domaines, et que ces noms « marcheront », c'est-à-dire qu'ils seront proprement publiés dans le DNS (*Domain Name System*, le protocole par lequel les noms de domaines sont utilisés).

Cette intervention d'une organisation unique fait peser une lourde pression politique sur le registre. Sa légitimité doit être établie (par exemple, par la loi), ses décisions vont être contestées et il y aura même des interrogations sur son éventuel remplacement (que l'on songe aux nombreux débats sur la gouvernance de la racine du DNS).

Un second type de service potentiellement « blockchainisable » est le « journal ». Un journal (« log », pensez au journal de bord d'un navire) est une suite d'informations dont l'ordre est important et qui ne doit pas être modifié, une fois écrit. Là encore, la sagesse conventionnelle était qu'il devait être tenu par une organisation unique en garantissant l'intégrité.

Il existe bien sûr beaucoup d'autres services qui sont tout aussi « blockchainisables » (comme Twister, concurrent de Twitter, mais entièrement pair-à-pair), mais qui ne font pas partie de ce que l'on peut appeler l'infrastructure de l'Internet.



Name d/mines (mines.bit)

Summary

Current value

Status Active
Expires after block 372084 (33483 blocks to go)
Last update 2017-04-08 18:20:34 (block 336084)
Registered since 2012-09-12 01:43:11 (block 74419)
First registration 2012-01-17 01:59:11 (block 38415)

Operations

Date/time	Block	Transaction	Operation	Value
2017-04-08 18:20:34	3360844	b8d2919ca...	OP_NAME_UPDATE	
2016-09-09 09:53:51	30416066	cc4d33db...	OP_NAME_UPDATE	
2016-02-01 15:07:29	270342	d03145b60c...	OP_NAME_UPDATE	
2015-07-29 12:28:11	2415870	da2d80f8d...	OP_NAME_UPDATE	
2014-12-08 09:33:52	2088985	f79bdc8d1...	OP_NAME_UPDATE	RESERVED
2014-05-16 06:30:06	1771103	e1db8618d...	OP_NAME_UPDATE	RESERVED
2013-10-26 00:08:12	142178	c02214eee3...	OP_NAME_UPDATE	RESERVED
2013-04-23 02:48:05	10727985	886c296b...	OP_NAME_UPDATE	RESERVED
2012-09-12 01:43:11	74419	f4328426d6...	OP_NAME_FIRSTUPDATE	RESERVED
2012-08-26 06:39:18	71754	6a2307d4fa...	OP_NAME_NEW	5180876b9d64a110b1e319d8b1124ac373b5dd53

History

Date/time	Block	Transaction	Operation	Value
2012-01-17 01:59:11	38415	11fba30995...	OP_NAME_FIRSTUPDATE	{"map":{"":"1.2.3.4"}}
2012-01-11 18:06:45	37558	d3f1e60452...	OP_NAME_NEW	1da7c76a9419690d04a475e93c4487833190b7df

« Blockchainiser » les registres

La chaîne de blocs permet d'obtenir un consensus entre des acteurs qui ne se font pas confiance, un consensus sur un état (par exemple, sur le contenu d'un registre). Le point important, dans cette définition, est : « entre des acteurs qui ne se font pas confiance ».

Si tous font confiance à un tiers, les traditionnelles bases de données conviennent mieux (et c'est pour cela que des chaînes de blocs privées n'ont guère de sens).

Potentiellement, la chaîne de blocs permet de remplacer complètement un registre. Cela aurait l'avantage de mettre fin aux polémiques sur la politique du registre, voire sur sa légitimité. Avant d'étudier la différence entre théorie et pratique, voyons les moyens concrets de réaliser cet objectif.

Pour le cas d'un registre de noms de domaine, il existe depuis de nombreuses années une solution opérationnelle nommée Namecoin. Namecoin est un logiciel dérivé du code du célèbre Bitcoin, mais qui a sa propre chaîne de blocs (et donc ses propres mineurs et ses propres explorateurs). Les auteurs ont ajouté au code la possibilité d'effectuer un nouveau type de transaction : l'enregistrement de noms et l'association de données à ces noms (de même que le DNS permet d'associer des données, comme les adresses IP, à des noms de domaine). Namecoin est parfois présenté avec des formules raccourcies du genre « un DNS pair-à-pair », mais ces formules sont trompeuses : Namecoin n'a rien à voir avec le DNS, l'unique point commun étant que dans les deux cas, il s'agit de systèmes permettant de récupérer des données associées à un nom.

Namecoin a toutefois une passerelle permettant à des clients DNS traditionnels de résoudre les noms Namecoin en données *via* le TLD (non officiellement enregistré) « .bit ». Si votre résolveur DNS a été configuré pour résoudre le « .bit », vous pouvez accéder aux noms Namecoin depuis un logiciel ordinaire, comme votre navigateur *Web*.

Il existe d'autres logiciels de gestion de chaînes de blocs qui sont sans doute meilleurs, techniquement, que Namecoin. C'est le cas d'Ethereum qui, au lieu d'imposer de modifier le logiciel de la chaîne pour chaque application différente, permet de faire exécuter des programmes quelconques par la chaîne de blocs. On peut ainsi écrire un logiciel de registre et le déployer sur la chaîne Ethereum commune. Un tel logiciel avait d'ailleurs été présenté en détail par l'auteur de ces lignes à la Journée du conseil scientifique de l'AFNIC, en juillet 2016. En voici une version simplifiée, écrite dans le langage Solidity :

Et c'est quasiment tout ! C'est la chaîne de blocs qui assure les fonctions essentielles, comme celle d'ordonner les demandes pour réaliser le « premier arrivé, premier servi ». Donc, un registre de noms sur la chaîne de blocs est parfaitement réaliste et, d'ailleurs, plusieurs existent déjà (comme EtherID ou Ethereum Name Service). Mais voyons les limites. D'abord, il faut noter que la chaîne de blocs ne permet pas de changer facilement la politique d'enregistrement en cours (à moins qu'il n'existe un mé-

canisme permettant qu'un acteur de confiance le fasse, mais, dans ce cas, on est presque revenu au registre traditionnel, justement ce que beaucoup de promoteurs de la chaîne de blocs voulaient éviter). Si cette politique d'enregistrement est « premier arrivé, premier servi », il ne sera donc pas possible de mettre en œuvre une politique d'enregistrement plus restrictive. La plupart des promoteurs de registres fondés sur la chaîne de blocs voient d'ailleurs cela comme un avantage : la chaîne est à l'abri de l'arbitraire et des passions (notons qu'elle a bien une politique, mais c'est celle définie au lancement, et généralement on ne peut pas la modifier). Il faut juste être bien conscient de cette caractéristique.

Ainsi, la chaîne de blocs ne conviendrait sans doute pas pour l'allocation d'adresses IPv4, une activité dans laquelle, en raison de l'ancienne pénurie, on ne peut allouer de nouvelles adresses qu'après un strict examen. Or, la chaîne de blocs ne sait pas gérer des ressources rares.

De même, pour le cas de la racine du DNS (citée plus haut), la chaîne ne pourrait pas facilement limiter le nombre de nouveaux TLD (domaines de premier niveau, comme « .re », .com ou « .pizza »). Si l'on voulait résoudre les actuels problèmes de gouvernance de la racine en passant celle-ci sur une chaîne de blocs, on aurait une dynamique de création de TLD très différente de l'actuelle.

Notez également l'absence de recours, la chaîne de blocs étant conçue pour fonctionner automatiquement, sans intervention humaine. Si vous perdez un nom de domaine traditionnel (par exemple, parce que vous avez oublié de le payer et que, redevenu libre, il a été pris par un tiers), vous avez des mécanismes de recours auprès du registre (ou de la justice). Ces mécanismes peuvent être lents, compliqués et chers, mais ils existent. Si vous perdez un nom enregistré *via* le programme qui tourne sur la chaîne de blocs, il n'y a pas de recours : vous ne pouvez pas argumenter avec… un algorithme ! (Une telle mésaventure était survenue à l'auteur de cet article en septembre 2015, et elle explique pourquoi le nom bortzmeyer.bit ne marche plus…). La sécurité de vos noms, sur la chaîne de blocs, repose sur une bi-clé (dont une partie est privée et l'autre publique) cryptographique. Comme son nom l'indique, la partie privée doit être gardée rigoureusement secrète. Si elle est copiée par un tiers, celui-ci pourra faire ce qu'il veut avec vos noms (vu le nombre de logiciels malveillants qui tournent sur n'importe quelle machine Microsoft Windows, le risque n'est pas purement théorique). Si la partie privée de la clé est perdue (pas de sauvegarde, et le disque dur qui tombe en panne…), vous ne pouvez plus modifier vos noms, voire vous ne pouvez plus les renouveler.

Là encore, pas de recours auprès d'une institution (comme il peut y en avoir si vous oubliez le mot de passe d'accès à votre Bureau d'Enregistrement). Or, l'expérience de la cryptographie acquise jusqu'à présent nous enseigne que les utilisateurs ne sont pas de bons gestionnaires de clés cryptographiques. Dans le futur, des solutions technologiques (comme des dispositifs matériels durcis stockant la clé privée) limiteront (peut-être) les risques, mais ne les supprimeront pas totalement.

« Blockchainiser » les journaux

Et les journaux, est-il intéressant et possible de les faire passer sur la chaîne de blocs ? Il existe déjà des journaux publics, comme les journaux de certificats X.509 utilisés dans le cadre du projet *Certificate Transparency*. L'idée, normalisée dans le RFC 6962, est que les Autorités de Certification (AC) publient dans un journal les certificats qu'elles signent. Ce journal ne permet que les ajouts, jamais de modifications ou de retraits. Le navigateur *Web* peut alors vérifier, lorsque le certificat lui est présenté par le serveur, que le certificat a bien été publié dans le journal. Et les titulaires de noms de domaine peuvent examiner en permanence le journal afin de s'assurer qu'il n'y a pas eu signature de faux certificats (le projet *Certificate Transparency* est promu par Google, ce qui est logique puisque cette entreprise a souvent été victime de l'émission de faux certificats ; on a vu, par exemple, des gouvernements faire faire par une AC nationale de faux certificats gmail.com, pour pouvoir intercepter le trafic avec ce serveur).

Les journaux actuels sont gérés par des entreprises qui limitent l'écriture aux AC « reconnues ». Pourrait-on les « blockchainiser » ? Certainement, et cela supprimerait la dépendance vis-à-vis d'un acteur privé. Mais, aujourd'hui, il semble qu'il n'existe pas de projet concret allant dans ce sens.

Conclusion

Alors, verra-t-on le remplacement des actuels registres, qui jouent un rôle si important dans l'infrastructure de l'Internet, par des chaînes de blocs ? D'abord, rappelons-nous que le choix n'est pas binaire. Il n'y a pas forcément le seul registre traditionnel, d'un côté, et le système complètement pair-à-pair, de l'autre.

On pourrait ainsi imaginer des solutions organisationnellement innovantes, comme une chaîne de blocs, mais avec l'existence de « notaires » qui assureraient pour leurs clients des fonctions difficiles, comme la supervision de la chaîne de blocs ou la gestion des clés cryptographiques. Un tel système aurait pour avantage que le titulaire de nom aurait une liberté complète quant au choix de son notaire (il aurait aussi celle de s'en passer).

Découpler les différentes fonctions d'un registre a en outre l'avantage intellectuel de faire réfléchir sur le travail des registres. J'ai donné une version très simplifiée de ce travail plus haut. Par exemple, je n'avais pas parlé de la sauvegarde des données, une fonction essentielle (dans la chaîne de blocs, les données sont automatiquement dupliquées, mais si tous les nœuds de la chaîne disparaissent, les données sont perdues. Or, Namecoin est une petite chaîne que maintiennent quelques enthousiastes).

Mais évidemment, le plus gros défi pour la chaîne de blocs sera celui de son adoption. Namecoin existe depuis des années. Or, il n'a jamais eu de succès. Plusieurs de ses services associés (comme les résolveurs DNS publics pour « .bit ») n'existent plus. Aujourd'hui, tout le monde peut, techniquement parlant, créer sur Ethereum un registre de noms en très peu de temps et avec peu de compétences (c'est le côté, très important, « sans permission » de l'Internet).

Mais ce registre sera-t-il reconnu par les utilisateurs ?

MakerNet : la fabrication distribuée

Par Pierre-Alexis CIAVALDINI
Étudiant-entrepreneur à l'École 42 et cofondateur du BlockFest
www.makernet.org

"*Release early, release often !*". Cet adage bien connu du monde informatique est issu de *The Cathedral and the Bazaar* (1) (1997), un des ouvrages fondamentaux du mouvement *open source* qui révèle l'avantage compétitif qu'offre cette nouvelle vision de l'informatique. Applicable au matériel, cette philosophie permet l'élaboration d'un nouveau modèle de fabrication distribuée sécurisable grâce à la *blockchain*. La France a délocalisé son industrie de pointe et a perdu une grande partie de son savoir-faire en micro-électronique. *A contrario*, à Shenzhen, en Chine, l'électronique est désormais une forme d'artisanat. Elle permet à la Chine de créer chaque jour des dizaines de nouveaux *smartphones* que l'on appelle des « *Shanzai* », une forme d'*open hardware* standardisé (qui n'existe que là-bas). MakerNet (2) propose la généralisation de ce modèle et son ouverture aux autres cultures au travers d'un écosystème de fabrication distribuée permis par la *blockchain*.

De l'*open source* à l'*open hardware*

L'histoire de l'*open source* commence le 1er janvier 1970 à minuit : c'est la Seconde 0 du Temps Unix ; cette date marque le début d'une nouvelle ère. Alors que le système d'exploitation Unix (créé par AT&T) n'a pas pu être commercialisé à cause d'une clause de non-concurrence, ses sources sont distribuées gratuitement. Des centaines de programmeurs contribuent au code source d'Unix, jusqu'à inspirer Richard Stallman, qui crée le projet GNU en 1984 (la première suite de logiciels totalement libre de droits). En 1991, le projet s'allie au noyau Linux pour proposer le premier système d'exploitation complet libre de droits. Il existe aujourd'hui des centaines de distributions GNU/Linux pour des usages encore plus variés que ceux des deux célèbres systèmes d'exploitation propriétaires Windows et MacOS.

Le produit lui-même étant rarement commercialisable, il est très difficile de tirer une loi générale des *business models* des industries de l'*open source* ! En revanche, son versant matériel, l'*open hardware*, semble être aujourd'hui extrêmement prometteur. Les plans des produits *open hardware* sont certes librement disponibles, mais il y a toujours un objet physique à vendre, ce qui rend plus facile la formalisation de son marché. Certes, on pourrait avancer l'idée qu'il reste toujours possible de « voler » le plan gratuit du concepteur pour pouvoir fabriquer en masse, mais ce serait sans compter sur la puissance de mise à jour que permet d'atteindre l'*open source*, grâce à une communauté d'intérêts. Ses membres participent à l'amélioration du produit pour que celui-ci comble réellement leurs attentes à une cadence que les usines de production de masse ne peuvent espérer suivre.

Considérés comme l'usine du monde, des fabricants centralisés (comme Foxconn et ses 1,6 million d'employés) sont capables de produire en masse des objets identiques, mais, dans un tel cas, toute modification de la chaîne de production est extrêmement onéreuse.

À l'inverse, une production reposant sur l'impression 3D est très bon marché. Tout comme Unix, la mise en libre-service des imprimantes 3D a fait leur succès actuel. Inventées en 1984 par trois Français pour Alcatel, c'est en 2004 qu'elles tombent dans le domaine public et que le projet *open hardware* RepRap donne naissance à des centaines de modèles.

Du prototypage rapide à la production industrielle

De plus en plus utilisées pour le prototypage rapide, les imprimantes 3D ne permettent pas, toutefois, de proposer une production de masse. Leur entretien est complexe et leur rapidité d'exécution reste pour l'instant faible. En les mettant en réseau, il serait en revanche possible de créer un *cluster* d'imprimantes 3D ayant une force de production remarquable : si une imprimante tombe en panne, cela occasionne peu de répercussions sur la chaîne de production ; comme un nœud d'une *blockchain*, une autre imprimante 3D prendrait le relais. Il en va tout autrement si un moule d'injection, coûtant plusieurs dizaines de mil-

(1) RAYMOND E. S., The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary, *O'Reilly Media, Würzburg, 1997-1999.*
(2) https://makernet.org/

liers d'euros faisait défaut dans une chaîne de production traditionnelle.

La fabrication additive est aujourd'hui principalement liée à l'*open hardware* et s'est heurtée à des problématiques légales sans précédent : que se passe-t-il lorsqu'un amateur reproduit une pièce soumise à brevet et la diffuse librement sur Internet ? De tels cas ont jusqu'ici été relativement isolés et sans grande ampleur. Il demeure cependant évident que l'industrie du brevet doit se saisir de cette question, comme c'est le cas actuellement dans le domaine de l'industrie créative, du fait de l'apparition de nouveaux modes de consommation.

Les *smart contracts* apportent un élément de réponse à ces questionnements. Par leur nature immuable, intègre et internationale, ils pourraient constituer un nouveau type de brevet numérique.

La fabrication distribuée

Internet offre tout un univers d'expérimentations aux secteurs de la production. Pourquoi transporter des produits à des milliers de kilomètres en consommant inutilement des centaines de litres de carburant, quand on peut faire transiter uniquement les informations concernant ces produits ? La constitution d'un réseau international de *designers* dont les produits sont manufacturés localement, à proximité de leurs acheteurs, est une utopie en passe de devenir réalité.

FabCity, un programme de politique urbaine créé en 2014 par Tomas Diez, marque un tournant dans les objectifs politiques des métropoles mondiales [3]. Ce projet a pour vocation de rendre ces grandes villes à 50 % autosuffisantes dans les domaines de l'énergie, de l'alimentaire et des produits industriels à l'horizon des quarante ans.

L'échange d'informations entre les métropoles sur leur production et leur consommation fait de ces villes les nœuds d'un réseau mondial qui apprend de ses usages et de ses différences. C'est à la problématique de l'autosuffisance de la production industrielle que MakerNet (qui est partie prenante de FabCity) s'est attachée à répondre.

MakerNet est une place de marché pour la fabrication locale et distribuée : elle met en relation *designers*, fabricants et consommateurs sur une plateforme proposant un ensemble d'outils pour la protection et la rémunération d'une propriété intellectuelle participative, en rassemblant ses différents acteurs en communautés d'intérêt autour d'un usage. L'objectif est de créer une base de données de communs matériels (à l'instar de Github [4], pour les logiciels).

Trois profils d'utilisateurs

Le terme de « *designers* » dans cet écosystème est à comprendre en son sens le plus large, celui d'inventeur. Le *designer* identifie un besoin d'usage et crée les plans de fabrication du produit qui y répond au sein d'une *blueprint*. Sa propriété intellectuelle est protégée et rémunérée grâce à la *blockchain*. Ce système l'incite à rendre ses plans de fabrication modulaires afin que d'autres projets puissent intégrer son travail. De fait, plus son travail est intégré dans celui d'autres *designers*, plus grande sera son assiette de droits à collecter lors de la fabrication des produits.

Fabriques et fabricants sont référencés sur MakerNet. *Hub* d'accès aux capacités productives et créatives d'une localité, cette plateforme promeut l'artisanat et les pro-amateurs [5]. Ces derniers sont capables de proposer une fabrication à la demande à moindre coût. Les fabricants sont certifiés sur leurs compétences par des *tokens* [6] qui leur sont décernés sur la *blockchain*. Ces *tokens* leur permettent de recevoir une requête de fabrication de tout ou partie d'un produit, à laquelle ils répondent par un prix de fabrication et un temps de livraison au prochain maillon de la chaîne de fabrication. Leur réputation est capitale s'ils veulent garder une bonne visibilité sur le marché.

Utilisateur final (et acheteur du produit), son consommateur, commande sur MakerNet la fabrication locale d'un produit. Il choisit un plan de fabrication qui génère un appel d'offres s'adressant aux fabricants certifiés autour de chez lui. Le consommateur reçoit alors une liste des routes de fabrication possibles pour la matérialisation de son produit. Son choix dépend du prix total du produit, de la qualité attendue, des matières proposées et du trajet parcouru par chacun des composants du produit.

Ces trois profils d'utilisateurs sont totalement perméables. Lors du prototypage d'un produit avant sa mise sur le marché, un utilisateur peut devenir tour à tour *designer*, fabricant partiel et consommateur de son propre produit, cette facilité de prototypage accélérant très fortement l'arrivée sur le marché d'un produit fini. Les *start-ups* sont ainsi à même de « palper » leur marché avant même de lever et de dépenser des fonds pour parfaire leur produit.

La rétribution des communs créatifs

Sur MakerNet, il est possible de créer une version modifiée d'un produit : comme sur Github, cela s'appelle un « *fork* ». Cette fonctionnalité est régie par les règles définies par le créateur du produit initial, par la licence qu'il lui a accordée et par le modèle de *business* qu'il a choisi (gratuit, donation libre, donation contre contribution, prix fixe, pourcentage du prix de production...). Cela a pour effet de créer un nouveau produit qui inclut la totalité de la propriété intellectuelle préexistante et leurs ayants droit. Lorsque ce nouveau produit sera fabriqué, le prix de la

(3) Les localités et les États ci-après ont déjà rejoint FabCity : Barcelone, Boston, Somerville, Cambridge, Ekurhuleni (Afrique du Sud), le Kerala (Inde), la Géorgie, Shenzhen, Amsterdam, Toulouse, la Région Occitane, Paris, le Bhoutan, Sacramento, Santiago de Chile et Detroit.

(4) GitHub est un service Web *d'hébergement et de gestion de développement de logiciels utilisant le logiciel de gestion de versions libre et décentralisé Git.*

(5) MILLER P. & LEADBEATER Ch., The Pro-Am Revolution: How Enthusiasts are Changing Our Society and Economy*, Londres, Demos, 2004.*

(6) Un token *est un jeton virtuel (sur une* blockchain*), dont la représentation dépend du système dans lequel il est utilisé (il peut, par exemple, signifier un droit d'accès ou encore un diplôme).*

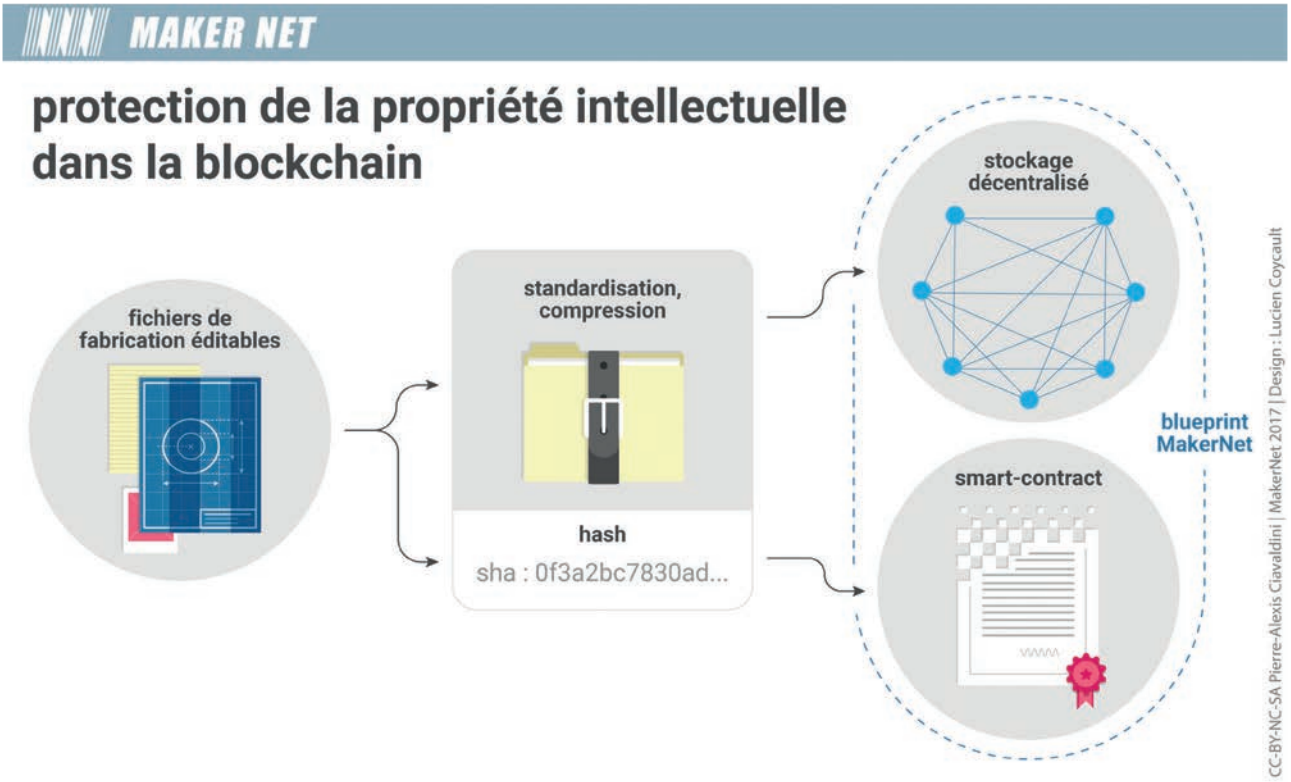


Figure 1

propriété intellectuelle sera calculé pour chacun en fonction de sa contribution à la création du nouveau produit.

Sur MakerNet, tout produit a donc nécessairement un marché associé, fût-il composé d'une seule personne. Lorsqu'un produit est « *forké* », son usage est modifié et il peut alors toucher une audience plus large. Ainsi, le *designer* du produit originel touchera les droits sur un marché plus large que son marché initial : les marchés de niche sont de ce fait dynamiques et ils s'agrandissent au fur et à mesure de l'amélioration d'un produit. Lorsque le *designer* effectue une mise à jour de ses plans de fabrication, un nouveau *blueprint* du produit est créé. Cette nouvelle version est sélectionnée par défaut pour la fabrication (mais les versions préexistantes demeurent accessibles). Ainsi, les mises à jour sont disponibles instantanément pour la fabrication dans le monde entier. Les consommateurs ayant déjà acheté le produit avant la mise à jour en sont notifiés : ils peuvent faire fabriquer la pièce mise à jour afin de remplacer la pièce obsolète, ou bien faire remplacer celle-ci par un fabricant.

La certification pair-à-pair

Pour assurer plus de confiance au sein de la communauté, un système de certification des compétences pair-à-pair est associé à des mécanismes de réputation. Prenons l'exemple du responsable d'une usine détenant une machine de découpe laser. Son usine référençant cette machine sur MakerNet, il peut certifier la compétence des personnes qui fréquentent sa fabrique en leur décernant le *token* de « compétence découpe laser ». Cela leur permet de recevoir des commandes locales de découpe laser.

Le fait de détenir ce *token* permet au certifié d'enseigner à son tour la « compétence découpe laser » à d'autres personnes et de certifier celles-ci. Ainsi, quand ces nouvelles personnes certifiées réaliseront des découpes laser sur MakerNet, un pourcentage de leur bénéfice sera reversé à leur professeur. Cependant, s'il s'avère qu'un fabricant fait mal son travail, deux réputations sont mises en cause : la sienne propre, et celle de son professeur sur cette compétence.

En résumé : les *designers* peuvent trouver des profils triés par certification de compétences. Les fabricants sont référencés par les *tokens* qu'ils détiennent, tandis que les *designers* sont référencés par les logiciels qu'ils utilisent pour former les *blueprints* qu'ils ont publiés sur MakerNet.

Pour proposer un produit sur la plateforme, le *designer* doit créer un *blueprint*. Un *blueprint* est la représentation virtuelle du produit et de son processus de fabrication, ceux-ci étant sécurisés sur une *blockchain*.

Les fichiers contenus dans le *blueprint* sont dans le format éditable des logiciels que le *designer* utilise. Ils sont standardisés, compressés et « hachés » pour former une archive complète du produit à fabriquer. Le fichier compressé est hébergé sur un stockage décentralisé (tel que BitTorrent) afin d'en assurer la disponibilité. Son *hash* est stocké dans un *smart contract* horodaté qui contient les adresses de paiement de tous les participants de cette propriété intellectuelle. Une fois stockée, le *blueprint* assure l'intégrité de son contenu : il est impossible de l'altérer. Il est néanmoins possible, en cas de litige, de révoquer le *blueprint.*

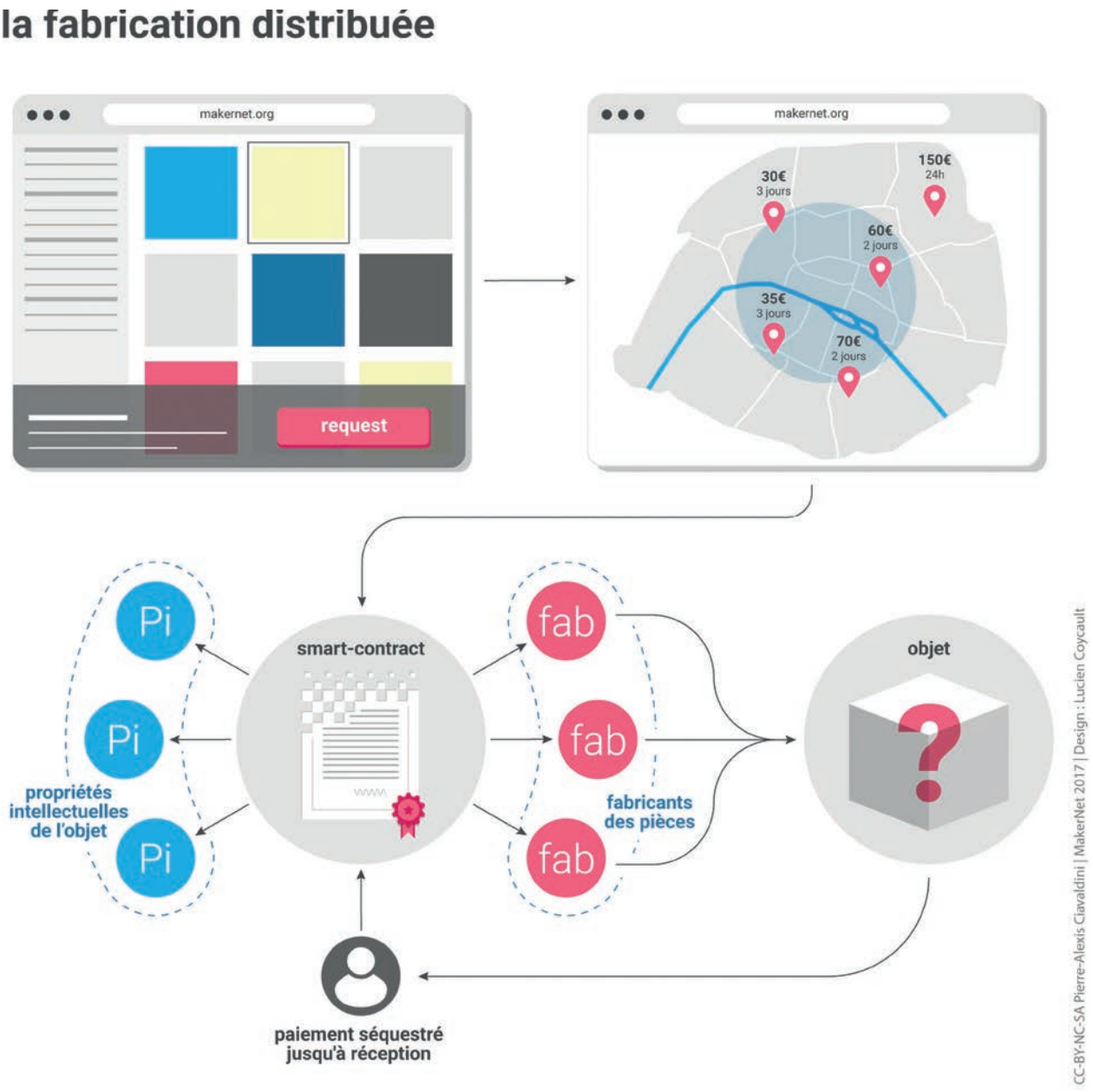


Figure 2

Sur MakerNet, le consommateur choisit son produit dans la liste des *designs* proposés et lance un appel d'offres aux fabricants locaux référencés par leur *token* certifiant. Ces derniers disposent d'un délai pour répondre à l'appel d'offres. MakerNet calcule alors les étapes de fabrication en fonction des offres, puis il propose celles-ci au consommateur, dès qu'elles sont disponibles.

Chaque route de fabrication inclut les prix des matériaux, du transport, de la fabrication et de la chaîne des droits de propriété intellectuelle. Optionnellement, elle peut intégrer les assurances et les normes de conformité. Lorsqu'une route de fabrication satisfaisante est constituée, le consommateur peut sélectionner celle-ci et en payer la réalisation. Son argent est sécurisé par un séquestre [7] sur le *smart contract* de la route de fabrication (seule la partie correspondant aux matières premières est envoyée aux fabricants ayant transformé ces dernières).

Le consommateur est assuré qu'il recevra son produit, car le reste de son paiement ne sera pas transmis aux fabricants tant que sa commande n'aura pas été délivrée (elle doit être conforme aux plans). Les fabricants sont, quant eux, assurés que le consommateur a déjà payé et que la somme qu'il a versée est conservée sous séquestre.

Après la livraison, en cas de litige sur la qualité du produit, le consommateur et le fabricant responsable de la partie défectueuse doivent trouver un arrangement amiable, à

(7) Un séquestre dans le domaine du droit est la procédure par laquelle un tribunal décide de placer un bien ou une somme d'argent sous la garde de la justice, rendant le bien séquestré momentanément indisponible pour son propriétaire, et ce, jusqu'au jugement qui y mettra un terme.

défaut de quoi le capital du *smart contract* comprenant le contrat de dépôt du client serait détruit [8].

La *blockchain*, levier de confiance

Bien qu'elle crée de l'emploi dans les domaines de la recherche et du développement, la robotisation générale a tendance à anéantir bon nombre de tâches et de métiers, notamment de métiers manuels.

Pour renouveler le système de production et de consommation actuel, nous proposons de placer l'innovation participative et l'artisanat – électronique inclus – au centre du schéma productif, grâce à la fabrication distribuée. Cette manière d'envisager la production industrielle est traversée de problématiques complexes. Notamment, un écosystème tel que celui-ci ne semble réalisable que grâce à la sécurité, à la dématérialisation monétaire et à la décentralisation intrinsèque apportées par la technologie *blockchain*.

En promouvant l'industrie pédagogique, les citoyens peuvent reprendre le pouvoir sur la technique et proposer des produits dont l'usage leur est adapté, au lieu de s'adapter à l'usage du produit.

Cet article a été mis au point avec la précieuse participation de Vivien Roussel et de Laura Bui.

*(8) Le contrat de dépôt est une somme supplémentaire à la commande qui ne sera pas restituée au client si un litige ne trouve pas de résolution. Ce principe repose sur celui de l'*ultimatum game*, expérience économique développée en 1982 par Güth, Schmittberger et Schwarze.*

Les Matrices de l'École 42*

Pas de cours, pas de profs : à l'École d'informatique 42, ce sont les étudiants eux-mêmes qui sont en charge de leur réussite et de la réussite de leurs camarades. Pour progresser sur les projets qui leur sont proposés, ils doivent compter sur la force du groupe, donner et recevoir des informations, être tour à tour formateur et apprenant. Ce mode d'apprentissage pair-à-pair supprime les liens de subordination dans l'apprentissage. Chacun est le garant d'une partie de la réussite de projets menés à bien ensemble.

« Nous passons de l'ère industrielle à l'ère digitale »

Créer, innover et construire sont les maîtres-mots de notre époque et les technologies rendent ces pratiques de plus en plus accessibles. L'École 42 enseigne à ses élèves à apprendre ces technologies par eux-mêmes (cependant, l'apprentissage autodidacte de l'informatique ne s'accompagne pas naturellement d'une maîtrise du monde institutionnel : entre ces deux univers, un dialogue productif reste à organiser).

Matrice est née de la rencontre entre 42 et Creative Valley (espace d'innovation et incubateur de *start-ups*). Ce programme met des institutions ou des entreprises en relation avec des étudiants de différentes filières pendant dix mois pour mettre au point des solutions numériques qui soient économiquement viables.

En conciliant l'agilité des *start-ups* et la puissance de réflexion du monde estudiantin, Matrice couvre l'ensemble de la chaîne d'innovation, depuis la recherche fondamentale jusqu'à la mise en production. Le programme permet d'aller plus loin que la pédagogie en intégrant des données réelles de marchés, d'entreprises et d'utilisateurs.

Attirées par l'approche hors normes de 42, plusieurs entreprises sont en passe d'intégrer le programme Matrice afin d'y étudier notamment des problématiques afférentes à la *blockchain*. La structure de l'école autorise les élèves à étudier, par intérêt personnel, des domaines qui sortent parfois des conventions. Motrice de l'apprentissage, cette curiosité intellectuelle est le gage d'un travail de qualité taillé sur mesure.

« Le numérique, veiller à ce qu'il ne dérive vers le seul ciblage publicitaire ou la prédation sur les données »

La place prépondérante que prend le numérique dans notre société contemporaine lui confère une puissance qui devrait l'astreindre à une constante remise en question morale. C'est pourquoi il est primordial d'accompagner la construction éthique des étudiants en informatique en les confrontant à la réalité des mondes institutionnels et professionnels.

À 42, rien n'est imposé : personne n'est là pour « forcer » les élèves à venir. L'école leur permet de combiner leurs besoins en formation et leur envie de faire. C'est le seul véritable moteur de l'apprentissage et de l'engagement. Les étudiants s'intéressent spontanément à des technologies, soumettent de nouveaux sujets pédagogiques et créent des groupes d'intérêt comme l'association Blockchain 42. Des conférences et des événements peuvent aussi être organisés, c'est ainsi qu'est né le BlockFest – festival pédagogique des *blockchains*, en juin 2016 au sein de l'École 42.

Monté par une équipe passionnée par la transmission et le partage, le BlockFest a pour objectif d'être un espace-temps de construction collective, accueillant et fertile. Conférences, ateliers de prototypage de haute technologie avec de la pâte à modeler et des baguettes chinoises, cours de programmation et analyses *business* s'y côtoient pour former un objet à plusieurs entrées à destination des néophytes de l'Internet comme des experts en cryptographie.

Depuis, deux autres BlockFest ont été organisés et une vingtaine d'entreprises ont pu étudier la faisabilité de projets *blockchain* et les prototyper.

* Par Pierre-Alexis Ciavaldini, étudiant-entrepreneur à l'École 42 et cofondateur du BlockFest, avec l'aide de François-Xavier Petit, directeur du programme Matrice à l'École 42.

Blockchains et *Smart Contracts* : des perspectives pour l'Internet des objets (IoT) et pour l'e-santé

Par Philippe GENESTIER
Docteur en microélectronique chez Orange Labs
Loïc LETONDEUR
Ingénieur en Recherche et Développement, en fonction au sein d'Orange Labs
Sajida ZOUARHI
Ingénieure et doctorante en informatique et réseaux chez Orange Labs et au LIG (Laboratoire d'informatique de Grenoble INP)
Alain PROLA
Concepteur/développeur d'applications sur plateforme Androïd
et Jean-Marc TEMERSON
Ingénieur de recherche, responsable d'équipe et de projets au sein d'Orange Labs, aujourd'hui à la retraite

Du fait de l'utilisation croissante d'objets connectés (IoT) et de l'interconnexion de systèmes hétérogènes générant des myriades de données personnelles, notre société numérique se trouve confrontée à des défis nouveaux, qu'elle se doit de relever : administration décentralisée et composite de ces objets, résilience, respect de la vie privée dans l'accès aux données, traçabilité des usages...
La *blockchain* offre des réponses à ces défis :
- un fonctionnement décentralisé,
- des mécanismes de consensus permettant de concilier des intérêts divergents,
- une confiance répartie par la suppression du tiers de confiance unique.
De nouvelles opportunités émergeront au sein d'une nouvelle économie du partage basée sur des réseaux sociaux 2.0, dans lesquels humains et objets connectés interagiront de façon indifférenciée. La *blockchain* nous permet de créer des « ancres » entre le monde physique et le monde virtuel. C'est ainsi qu'une opération ou une transaction dans le monde réel pourra avoir son homologue dans le monde numérique.
Même si la *blockchain* ne répond pas à toutes les problématiques, ce type de solution est tout à fait pertinent dans des domaines où confiance, transparence et traçabilité sont indispensables. Néanmoins, il ne faut pas passer sous silence ce que la *blockchain* ne permet pas, notamment la vérification de l'authenticité des données enregistrées ou la vérification de la légitimité d'une opération « non électronique ».

Les possibilités offertes par la technologie *blockchain,* en particulier l'automatisation des transactions *via* des *smart contracts*, ouvrent un champ immense d'applications et de bouleversements organisationnels par la remise en question du rôle de certains acteurs, dans de nombreux domaines. Cela concerne en particulier des domaines comme l'Internet des objets (IoT, *Internet of Things*) ou la santé.

L'expansion rapide de l'Internet des objets dans notre monde numérique soulève des défis nouveaux. Tant pour leur gestion que pour la maîtrise des données qu'ils génèrent, ces objets connectés nécessitent des approches innovantes. Des technologies comme la *blockchain* permettent de relever tout ou partie de ces défis, tout en engendrant des usages novateurs : en témoignent des acteurs tels que Filament, IOTA ou IBM Watson IoT.

Les 26 milliards d'objets connectés pressentis à l'horizon 2020 constitueront une armada de taille inédite à administrer et à exploiter. Les aspects de garantie de sécurité, de confiance, de transparence, de qualité de service et de respect de la vie privée sont des questions clés pour le développement de l'IoT. Ces mêmes questions se posent également dans le domaine de la santé, avec le développement des solutions de télé-suivi (basées ou non sur des objets connectés) et de dossiers médicaux numérisés dans des systèmes hétérogènes, pour lesquels des exigences réglementaires fortes existent (notamment en ce qui concerne la prise en compte du consentement des patients à un accès à leurs données). Les approches traditionnelles basées sur des plateformes centralisées et/ou sur le postulat d'une gouvernance de bout-en-bout seront inadaptées. Pour dépasser ces approches, la technologie *blockchain* pourrait apporter des éléments de réponse.

Les défis de l'Internet des objets

L'IoT concerne un environnement à la fois massif et géo-distribué. Pourtant, les réseaux verticaux, à l'instar de celui de la santé, exigent des performances à la fois élevées et prédictibles, notamment en termes de bande passante et de latence réseau. Ces exigences requièrent une disponibilité aussi grande que possible des plateformes IoT malgré un environnement défavorable, que celui-ci soit dû à des risques de défaillance qui se retrouvent à tous les niveaux – des objets eux-mêmes jusqu'aux infrastructures de *datacenters,* en passant par les éléments réseau –, à des risques dus à la malveillance – illustrés par le récent exemple du *malware* Mirai [1] – ou encore aux aléas climatiques.

En conséquence, les plateformes IoT doivent posséder des propriétés de résistance (capacité à maintenir un état fonctionnel lors d'une occurrence de panne) et de résilience (mise en place de stratégies visant à recouvrer un état fonctionnel).

Par ailleurs, d'autres éléments doivent être pris en compte, comme la nécessité de pouvoir passer à l'échelle face au grand nombre d'objets connectés, le silotage (indépendance des constructeurs et absence de normes conduisant à des sous-ensembles isolés, parfois non interopérables), la gouvernance (éclatée entre de nombreux acteurs), l'hétérogénéité (des matériels, des protocoles, des environnements de programmation et des formats d'échange) et la découverte des objets connectés.

Face à de tels enjeux, seules répondront des plateformes distribuant des capacités de communication, de traitement des données (accès, filtrage, agrégation, stockage) et d'administration au plus près des objets, à l'instar des plateformes de *Fog Computing* [2]. La *blockchain* apporte des solutions de choix pour réaliser ces plateformes, qui seront des systèmes intelligents multi-agents.

Les problématiques du domaine de l'e-santé

L'informatisation croissante du domaine de la santé (avec le développement du télé-suivi, celui des dossiers patients dans tous les organismes de soins ou encore la mise en place de projets sur la médecine personnalisée) génère des préoccupations croissantes en termes de respect de la vie privée, de sécurité, en plus des contraintes réglementaires à prendre en compte par les acteurs du secteur. En outre, l'aspect très éclaté des systèmes d'information médicaux et les besoins croissants d'interconnexions ou d'échanges de données entre ceux-ci nécessitent de lourds processus de prise en compte du consentement des détenteurs de données au partage de celles-ci avec plusieurs tierces parties. Par ailleurs, ces mêmes usages soulèvent la question de l'authenticité des données et celle des moyens permettant de s'en assurer. Au niveau des assurances médicales, il est souvent difficile d'avoir une information à jour en ce qui concerne les droits d'un assuré.

La technologie *blockchain*

La *blockchain* est une innovation technologique en matière de stockage d'informations. Elle permet de stocker de façon sécurisée des informations (chaque écriture est authentifiée, irréversible et répliquée) avec un contrôle décentralisé (il n'y a pas d'autorité centrale qui contrôlerait le contenu de la base de données).

Elle s'appuie sur des techniques cryptographiques (fonction de *hash* [3] et cryptographie asymétrique) et sur l'utilisation d'un réseau informatique de nœuds indépendants.

Les technologies de la *blockchain* proviennent initialement de la crypto-monnaie bitcoin, pour laquelle elles ont été utilisées afin de créer un historique fiable des transactions financières.

Il existe des mises en œuvre alternatives autour du principe de la *blockchain*, avec des variantes dans les permissions de lecture et d'écriture des informations (privées, publiques ou semi-publiques), dans les types d'informations stockées (transactions financières, registre de propriété...) et en matière de performances (7 tps [4] pour bitcoin contre plus de 1000 tps avec d'autres *blockchains* sans mécanisme de preuve de travail).

La technologie *blockchain* voit aussi apparaître des évolutions qui ouvrent de nouvelles perspectives : les *smart contracts* qui réalisent des transactions conditionnelles automatisées s'exécutant sans intervention humaine ni tiers de confiance ; les applications décentralisées qui utilisent la *blockchain* comme infrastructure pour s'exécuter sans plateforme informatique centralisée.

---

(1) Une attaque de type déni de service via *des caméras connectées a été menée en 2016.*
(2) Le Fog Computing *est un prolongement des concepts du* cloud computing *au plus près des utilisateurs : déport d'une partie des traitements dans les objets connectés eux-mêmes (montres, capteurs…) ou dans les passerelles qu'ils utilisent (LiveBox ou téléphone mobile…).*
(3) Le hash *consiste à calculer une signature numérique de longueur fixe sur un ensemble de données, de sorte que toute modification de ces données entraîne une modification de la signature.*
(4) TPS : transactions par seconde. Il s'agit d'un indicateur de performance qui se base sur le nombre de transactions qui sont validées par le réseau en une seconde.

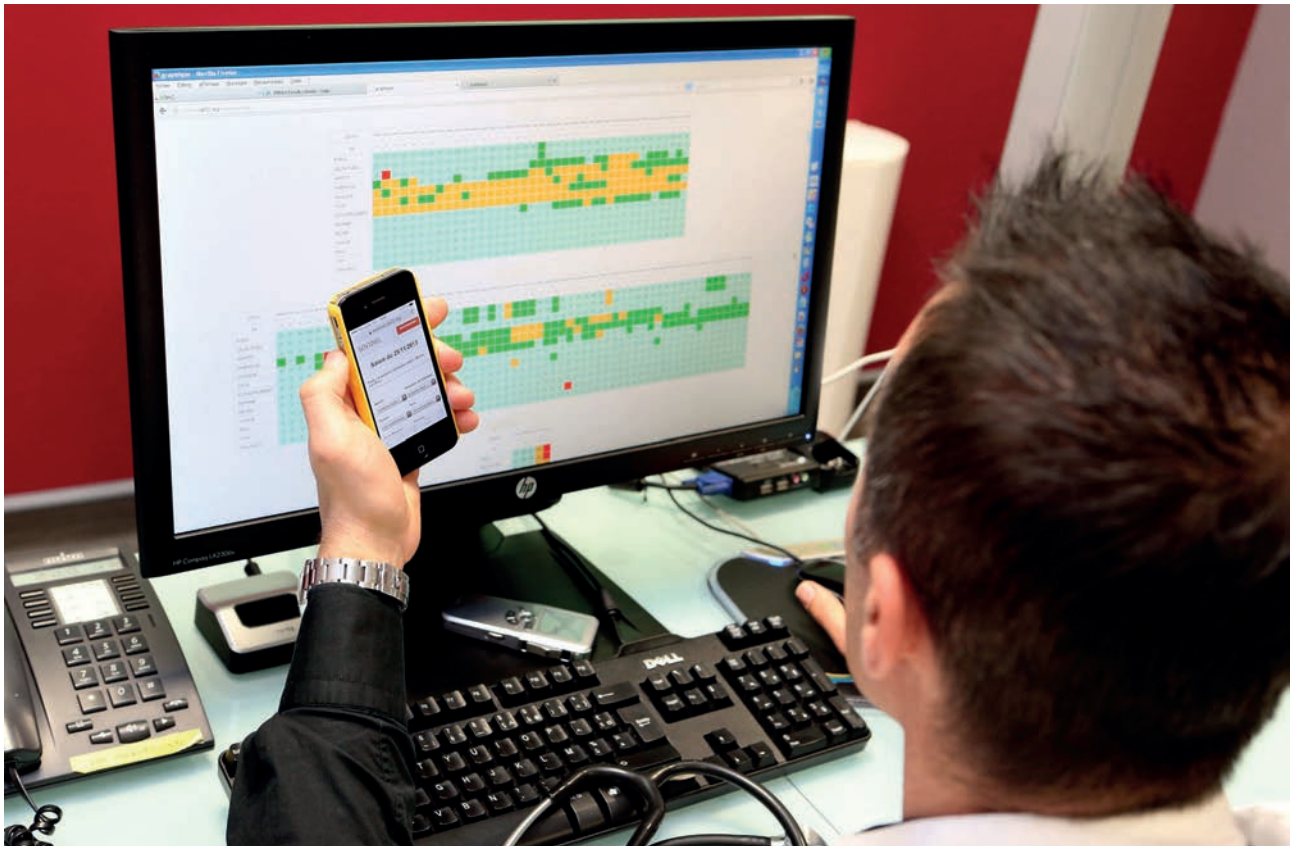


Photo © Bigot/ANDIA.fr

Recours au Centre Jean Bernard au Mans – Clinique Victor Hugo à une application utilisable sur *smartphone* inventée par Fabrice Denis, oncologue de l'établissement, pour dépister par anticipation les risques de récidive du cancer du poumon.

« L'informatisation croissante du domaine de la santé (avec le développement du télé-suivi, celui des dossiers patients dans tous les organismes de soins ou encore la mise en place de projets sur la médecine personnalisée) génère des préoccupations croissantes en termes de respect de la vie privée, de sécurité, en plus des contraintes réglementaires à prendre en compte par les acteurs du secteur. »

Les réponses apportées par la *blockchain* à l'Internet des objets

Si la *blockchain* ne fournit pas des réponses à tous les défis de l'IoT, elle apporte néanmoins un ensemble de fonctionnalités et de propriétés intéressantes qui pourraient constituer des éléments de choix pour les plateformes IoT.

L'IoT est par nature dynamique non seulement de par la mobilité des éléments qui le composent et de par les risques de défaillance, mais également en raison de son lien étroit avec la société de consommation mondialisée, où achats sporadiques de masse et obsolescence sont de règle. De ce lien découle une forte complexité liée à la découverte des objets connectés et des éléments d'infrastructure. Si tel objet s'avère légitime à un moment donné, il peut rapidement ne plus l'être, suite à sa revente ou à son vol, ou de par sa mise au rebut par les utilisateurs. Par ailleurs, il est nécessaire de protéger l'utilisateur contre des objets malveillants en interdisant la prise en compte. La solution *blockchain* permettra de légitimer les objets, de les répudier et de les bloquer en offrant un registre résistant et traçable d'autorisations liant le choix des utilisateurs finaux aux plateformes IoT. Une telle fonctionnalité est une extension de celle qui est connue sous l'expression de gestion de consentement et qui consiste à enregistrer les modalités de l'accès à ses données octroyé par un propriétaire à un tiers. Dans le cas présent, il s'agira pour le détenteur ou l'administrateur d'un objet de pouvoir en définir le statut (opérationnel, obsolète, en accès public…) d'une manière qui soit traçable et non répudiable.

Ces plateformes seront composées d'importants ensembles d'agents hiérarchisés capables d'exploiter et d'administrer des sous-ensembles de l'IoT. Du fait de la nature ultra-dynamique et hostile de l'IoT, ces agents entreront en conflit de décision et de responsabilité pour savoir qui est légitime pour décider d'actions sur les objets, l'infrastructure et les données, ou encore quelles sont les données et les fonctionnalités utilisables tout en préservant le respect du choix des utilisateurs et de leur vie privée.

La *blockchain* apportera par construction une solution de recherche de consensus à même de résoudre ces conflits en créant une autorité répartie, sécurisée, cohérente et traçable apte à vérifier toutes propriétés que les plateformes IoT devront posséder.

Plus généralement, la *blockchain* constitue une solution innovante en matière de délégation de droits pour rendre à un détenteur de données le contrôle de leur usage par des tiers, comme cela est imposé par la réglementation dans le domaine médical (en attestent les travaux en cours à ce sujet dans le cadre du Healthcare Data Institute et au sein d'Orange).

De cette communauté de besoins ont été identifiés plusieurs cas d'usage intéressant ces domaines et tirant parti des caractéristiques intrinsèques de la *blockchain* :

- la gestion du consentement [5], car celui-ci est au cœur des obligations réglementaires et des préoccupations pour le partage d'informations entre acteurs du monde de la santé : consentement du patient à la collecte et à la consultation de ses données par des soignants, ou encore à l'utilisation de ses données dans le cadre d'études cliniques. Dans le monde de l'Internet des objets, consentement du propriétaire d'un objet pour que les données issues de cet objet soient utilisées par des tiers (et définition des conditions d'utilisation), par exemple pour les diffuser ou les agréger avec d'autres ;
- la traçabilité des actions effectuées dans un système de collecte et de stockage de données ;
- la mise en œuvre de plateformes d'échange de données (par exemple, pour la mise en relation de donneurs et de receveurs d'organes[6]) ;
- le suivi de matériels tout au long de leur vie : production, transport, stockage et utilisation.

Rendre le pouvoir à l'utilisateur

Mise au service de l'IoT, et notamment dans des approches du type *Fog Computing*, la *blockchain* permet à l'utilisateur de gérer finement les droits d'accès à ses propres objets et données et leur utilisation par des tiers, ainsi que de journaliser les utilisations du patrimoine connecté des utilisateurs, tout en leur offrant une traçabilité ayant valeur de preuve en cas d'abus.

De ces deux atouts résulte une confiance renforcée des utilisateurs dans l'IoT face à l'aspect anxiogène de mythes errant de Big Brother en Skynet : la *blockchain* réaffirme leur gouvernance sur leur existence dans le monde numérique.

Au-delà de ses apports techniques, la *blockchain* pourra être le terreau d'une économie nouvelle laissant entrevoir de nouvelles sources de revenus. Par exemple, en facilitant l'émergence de réseaux sociaux 2.0, dans lesquels humains et objets connectés interagiront de façon indifférenciée au travers de transactions telles que l'achat de produits dont les deux types d'acteur auraient besoin (voir à ce sujet l'exemple développé par IBM et Samsung de machine à laver capable de commander de la lessive lorsque son stock est épuisé). Ces réseaux pourront être le support d'une économie collaborative rétribuant les possesseurs d'objets connectés en fonction de leur utilisation par d'autres membres du réseau, qu'ils soient humains ou objets. Cette économie s'inscrira pleinement dans le contexte actuel d'« ubérisation » et de déréglementation plaçant l'utilisateur comme fournisseur et « consommacteur » de biens et services. Par ailleurs, de tels réseaux sociaux seront une formidable source de création de valeur dans des perspectives de *Big data*.

La *blockchain* apparaît ainsi comme un facilitateur extraordinaire pour les plateformes IoT de demain (de type *Fog Computing,* par exemple), qui seront complètement décentralisées, offrant un service de qualité, fiable, traçable et maîtrisable par l'utilisateur final.

Les limites de la *blockchain*

Théoriquement apte à faciliter la transition en cours vers le monde IoT, la *blockchain* n'est cependant pas la solution miracle. Elle présente de fait quelques limites.

En premier lieu, elle n'assure ni la fiabilité des données remontées ni l'authentification des acteurs (qui consiste à s'assurer qu'une personne est bien celle qu'elle prétend être, par exemple à l'aide d'une solution comme Mobile Connect d'Orange), qui sont du ressort d'autres mécanismes. Une seconde limitation est relative au champ d'application de la *blockchain*, celle-ci ne concernant que des éléments (objets, événements…) ayant une « ancre » fiable dans le monde numérique, comme EverLedger a su le faire brillamment pour la traçabilité des diamants afin de lutter contre la contrefaçon. Un événement n'ayant pas de trace numérique ne pourra pas être pris en compte.

Ensuite, d'un point de vue technique, la *blockchain* fait un fort usage des technologies actuelles de *hash* et de chiffrement. Sachant que l'utilisation de certains registres créés au travers de la *blockchain* peut durer plusieurs dizaines d'années et que la fiabilité de la *blockchain* est basée sur celle de ses mécanismes intrinsèques, se pose donc une véritable problématique de pérennité de la protection des informations stockées face à la vulnérabilité future des algorithmes utilisés. En effet, un rapport du NIST (*National Institute of Standards and Technology*) pointe la vulnérabilité de ces algorithmes face à un ordinateur quantique (celui-ci pourrait exister dès 2030). Un tel ordinateur aura une puissance suffisante pour casser les protections mises en place aujourd'hui, et donc, en particulier, pour revenir sur des transactions passées.

Enfin, sur le plan juridique, la *blockchain* constitue une preuve « de fait » qui, en l'absence actuelle de qualification légale, n'est pas une preuve d'acte juridique.

Conclusion

Face aux nombreux défis posés par l'IoT et l'e-santé, et face aux besoins suscités en termes de décentralisation, de traçabilité et de confiance, la *blockchain* offre des réponses. Sans avoir la prétention de résoudre tous les problèmes, elle ouvre également la porte vers de nouveaux horizons. De ce fait, elle présente des champs d'investigation inédits aux acteurs du domaine, qui ne pourront faire l'économie de s'y intéresser.

---

(5) Blockchain for Consent Management in the eHealth Environment: A Nugget for Privacy and Security Challenges, *par GENESTIER Ph., ZOUARHI S., LIMEUX P., EXCOFFIER D., PROLA A., SANDON S. & TEMERSON J.-M. Publié dans* Journal of the International Society for Telemedicine and eHealth *(2017).*

(6) Plus d'informations sur le site officiel du projet Kidner : www.kidner-project.com

La régulation des *smart contracts* et les *smart contracts* des régulateurs

Par Catherine BARREAU
Professeur à la Faculté de droit et de science politique de l'Université de Rennes 1,
IODE UMR CNRS 6262, Université Bretagne-Loire

Tôt ou tard, toute innovation technologique est saisie par le droit. Le besoin de régulation est exprimé tant par les utilisateurs de l'innovation qui en tirent profit que par ceux qui pourraient en être victimes. Ainsi, les chaînes de blocs prennent discrètement place dans l'environnement légal, dans le domaine du financement des entreprises. Les *smart contracts*, dont les cas d'usage restent limités, devraient les rejoindre sous peu, la complexité de l'outil requérant un cadre juridique sécurisé pour permettre son développement. Réguler ce nouvel objet exige d'en déterminer la nature pour établir ses usages. Si ceux-ci sont essentiellement privés, un usage public par une autorité de régulation peut néanmoins être envisagé.

Le dilemme est toujours le même face à une innovation technologique : faut-il réguler ? Cette première question est suivie d'une seconde : comment la réguler ? La régulation institutionnelle [1], rapportée à des innovations technologiques, est souvent critiquée et presque toujours instable et lacunaire. Lorsque l'on s'intéresse à la chaîne de blocs et aux *smart contracts*, on s'aperçoit que la première a atteint la phase de régulation institutionnelle d'une manière telle que les seconds ne devraient pas y échapper, dans un futur proche, pour en assurer un développement harmonieux dans la sphère privée. Mais la sphère publique pourrait elle aussi tirer profit de cette innovation juridico-technologique. Objet de régulation, le *smart contract* pourrait lui aussi devenir un outil de régulation.

Le *smart contract*, objet de régulation

Le développement de la technologie dans le domaine de la finance d'entreprise a rendu pertinente l'adoption d'une régulation institutionnelle. Le projet de loi à l'origine de la loi Macron [2] prévoyait une habilitation du gouvernement par le Parlement à prendre, par ordonnance, toutes mesures nécessaires concernant l'adaptation du droit applicable aux titres financiers et aux valeurs mobilières afin d'en permettre la représentation et la transmission, au moyen d'un dispositif d'enregistrement électronique partagé. Cette disposition a été abandonnée, le rapporteur ayant estimé « douteuses » les habilitations pour donner un cadre juridique aux opérations de titres non cotés au moyen de *blockchains*. En conséquence, une ordonnance du 28 avril 2016 [3] a seulement créé des minibons, sur le modèle ancien des bons de caisse. Un décret du 28 octobre 2016 [4] a réglementé leurs conditions d'émission et fixé les modalités de leur transfert de propriété. Celui-ci « 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. À défaut, par dérogation aux dispositions de l'article 1323 de ce [même] Code [5], le transfert de propriété de minibons résulte de leur inscription au nom de l'acquéreur dans le registre prévu à l'article L. 223-4 ». Le registre de l'article L. 223-12 est défini comme étant un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations dans des conditions, notamment de sécurité, définies par décret pris en Conseil d'État [6]. Il s'agit d'un renvoi implicite à la technologie des chaînes de blocs, mais celui-ci demeure inefficace en l'absence de décret.

L'inquiétude subsistant chez les parlementaires, une question écrite a été posée : « lorsque la technologie aura été suffisamment développée et que du contentieux apparaîtra, les questions liées à la responsabilité des parties prenantes, les obligations du "fournisseur d'accès", le droit à l'oubli ou

(1) Soit le recours à la loi ou au décret par opposition à l'autorégulation ou à la corégulation.
(2) Loi n°2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques, dite loi Macron.
(3) JORF n°0101 du 29 avril 2016.
(4) JORF n°0254 du 30 octobre 2016.
(5) Cet article dispose : « Entre les parties, le transfert de la créance s'opère à la date de l'acte. Il est opposable aux tiers dès ce moment. En cas de contestation, la preuve de la date de la cession incombe au cessionnaire, qui peut la rapporter par tout moyen. Toutefois, le transfert d'une créance future n'a lieu qu'au jour de sa naissance, tant entre les parties que vis-à-vis des tiers. »
(6) Si l'on en croit la presse économique, les minibons en seraient à peine au stade de l'expérimentation, Les Échos, *mardi 30 mai 2017, p. 26.*

encore la protection du consommateur se verront opposer un vide juridique ». Son auteur souhaitait, dès lors, connaître les intentions du gouvernement afin d'ériger un véritable régime juridique de la *blockchain* [7]. En réponse, l'article 120 de la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique a habilité le gouvernement, d'ici au 9 décembre 2017, à réformer le droit applicable aux titres financiers afin d'en permettre la représentation et la transmission au moyen d'un dispositif d'enregistrement électronique partagé (*distributed ledger technology,* ou DLT) des titres financiers qui ne sont ni admis aux opérations d'un dépositaire central ni livrés dans un système de règlement et de livraison d'instruments financiers. Si la chaîne de blocs n'est pas seule concernée, elle a vocation à être le principal objet de la régulation financière envisagée [8]. Le gouvernement a lancé une consultation publique pour recueillir l'ensemble des avis des parties prenantes intéressées.

Deux enseignements peuvent être déduits. D'une part, le Code civil, siège par excellence du droit commun des relations entre parties privées, est applicable par défaut et il doit y être dérogé lorsque ses dispositions sont incompatibles avec la technologie développée. D'autre part, associer les destinataires de la réglementation à l'élaboration de la régulation paraît être de nature à renforcer leur capacité à mieux accepter celle-ci, si leurs attentes sont prises en compte. En outre, sur des sujets aussi complexes sur le plan technique, aucune expertise ne peut être négligée. Internet est un lieu de libre et égale expression et les technologies des chaînes de blocs et des *smart contracts* sont décentralisées : les personnes intéressées peuvent donc être particulièrement réactives. Cette méthode peut être dupliquée en vue de la régulation du *smart contract*.

Si le rapprochement entre le *smart contract* et les chaînes de blocs s'impose, il ne doit pas occulter le fait que le recours aux algorithmes permet déjà de profiter de la rapidité, de la simplicité et de la sécurité du numérique, et ce en dehors des dispositifs d'enregistrement électroniques partagés. Ces logiciels ne permettent que l'envoi d'une suite de notifications qui avertit chaque partie que son obligation doit être exécutée en lui rappelant son objet et sa date d'échéance. Les contrats conclus en faisant usage de ces logiciels obéissent aux conditions habituelles de validité des contrats posées par le Code (art. 1128). Le droit positif a été adapté pour faciliter le recours au numérique en permettant la conclusion d'un contrat par voie électronique (C. civ. art. 1125 et s.) et aucune autre régulation n'est nécessaire pour recourir à ces logiciels, qui peuvent en outre être dédiés à un modèle de contrat et faciliter le respect des conditions spéciales de validité de celui-ci. La dématérialisation des contrats permet la rédaction d'actes authentiques sur support électronique, mais le *smart contract* requiert des solutions plus technologiques.

L'expression *smart contract* renvoie à un dispositif plus sophistiqué qui permet l'exécution automatique des obligations enregistrées dès lors que les conditions d'exécution de ces engagements sont réunies, en prenant en compte l'ensemble des conditions et des limitations qui ont été programmées à l'origine dans le cadre du contrat. Aucune des parties ne peut s'opposer à l'exécution. Le coût et le ralentissement imputables à l'intervention du tiers de confiance sont supprimés. La technologie permet par elle-même de faciliter la conclusion du contrat entre des parties qui ne se connaissent pas, de s'assurer que chacune exécutera son obligation et d'enregistrer de manière fiable la transaction dans un registre, une sorte de grand-livre comptable, affirmé infalsifiable. L'ambiguïté de l'expression française a été d'emblée relevée : le *smart contract* n'est pas « intelligent », même si une couche d'intelligence artificielle est présente dans le programme informatique utilisé. Son « intelligence » tient à sa capacité d'auto-exécution des obligations contractuelles enregistrées. La qualification de contrat du *smart contract* mérite un examen plus détaillé, dans le cadre de cette réflexion sur sa régulation institutionnelle.

Si l'on considère que le *smart contract* est un contrat au sens de l'article 1101 du Code civil [9], deux possibilités sont envisageables. Si ce contrat est soumis aux règles du Code civil, il faut alors déployer des moyens considérables pour convertir toute la législation française en code informatique pour que le *smart contract* offre aux parties le bénéfice de toutes les dispositions juridiques et judiciaires protectrices habituelles. Des incompatibilités subsisteront. La chaîne de blocs est, par exemple, impossible à modifier. Par conséquent, en cas d'annulation du contrat, le retour au *statu quo ante*, le fait de réputer non écrites les clauses abusives ou la prise en compte de décisions de justice accordant un délai de grâce sont impossibles. La chaîne de blocs et le droit des contrats entreront en conflit. Il est certes possible de prévoir l'exécution immédiate d'une obligation monétaire destinée à compenser par équivalent l'impossibilité d'annuler ou de suspendre une obligation enregistrée qui a été exécutée correctement sur le plan informatique, mais de manière infondée en droit. Les principes directeurs du droit des contrats ne peuvent être maintenus. Il faut donc y déroger. En revanche, si ce contrat est exempté des prescriptions légales en vigueur par une loi dérogatoire, on peut imaginer que cette loi soit exprimée en code (informatique), et pas seulement en langage naturel. La dérogation pourrait être totale. Le *smart contract* serait alors doté d'une totale autonomie juridique. Cette démarche est susceptible de soulever deux difficultés : comment créer la confiance nécessaire au développement de cet outil ? L'usage de cet outil pourrait-il être ouvert à tous les contrats et à toutes les parties ? La dérogation pourrait consister à en proposer des adaptations : l'exigence de la certification de la signature électronique par un tiers de confiance (puisque la chaîne de blocs repose sur l'absence de tiers de confiance), la possibilité de renoncer par avance à toute action en justice, dès lors que le *smart contract* est conclu entre des personnes qui ne se connaissent pas (en raison de l'anonymat caractéristique de la chaîne de blocs)…

(7) Question écrite n°96014 du 24 mai 2016.
(8) http://www.tresor.economie.gouv.fr/File/434688
(9) Le contrat est un accord de volontés conclu entre deux ou plusieurs personnes qui est destiné à créer, modifier, transmettre ou éteindre des obligations.

Une autre possibilité est de considérer que le *smart contract* n'est pas un contrat. « Un *smart contract* peut être comparé à une feuille de papier. Celle-ci peut avoir une valeur juridique lorsqu'elle répond à l'ensemble des critères nécessaires pour être un contrat, mais seul le corpus juridique lui donne cette valeur. L'aspect intéressant de la chaîne de blocs, et d'une façon plus large du code, est qu'il est possible d'y implémenter des conditions qui s'appliquent automatiquement. Cependant, ces conditions sont limitées par le cadre technique, qu'il ne faut absolument pas confondre avec le cadre juridique. Il est possible de connecter l'un à l'autre, mais ce n'est pas le cas par défaut [10] ». La séparabilité du contrat, acte juridique, et du *smart contract,* mode d'exécution technique, semble compatible avec les pratiques actuellement constatées qui sont de nature à faciliter le développement du recours à la chaîne de blocs en matière contractuelle. Il suffit alors que les parties à un contrat valablement conclu en dehors de la chaîne de blocs conviennent, dans ce contrat, de recourir à un *smart contract* pour l'exécution de leur accord. Les principes directeurs du droit des contrats (liberté contractuelle, autonomie de la volonté, consensualisme et licéité des conventions sur la preuve) s'allient pour créer un cadre juridique assez souple et sûr. Les quelques usages constatés actuellement exploitent d'ailleurs ces principes. Quelle serait la régulation institutionnelle dans l'optique d'un *smart contract* reposant sur une chaîne de blocs publique ? Formellement, elle pourrait prendre place dans une sous-section 3 ajoutée à la section consacrée aux effets du contrat entre les parties [11]. Après celles consacrées à la force obligatoire et à l'effet translatif, le Code civil pourrait prévoir plusieurs dispositions confirmant la possibilité, pour les parties, de coder les obligations créées par le contrat conclu entre elles en vue d'assurer sa bonne exécution et aménageant les conséquences, sur la chaîne de blocs, de la nullité éventuelle du contrat ou de la reconnaissance du caractère abusif de certaines des clauses dudit contrat, en particulier de la clause prévoyant le recours au *smart contract*. Parmi les dispositions les plus importantes de cette sous-section, figurerait tout d'abord celle qui délimiterait le champ d'application du recours au *smart contract*. Il nous semble que seuls les contrats consensuels, créant des obligations ayant pour objet des prestations simples à exécuter et soumises à peu de conditions, conclus entre des parties disposant d'une puissance économique équivalente devraient ouvrir le recours au *smart contract*. Cela reviendrait à faciliter l'usage de ce recours aux professionnels qui contractent ensemble et aux interrelations des particuliers. Les ventes d'immeubles, les contrats de prêts bancaires notamment, ne devraient pas permettre le recours à la chaîne de blocs : la déception sera grande pour les *start-upers* qui souhaitent déjà « disrupter » ces activités, mais le système actuel repose sur des bases sociétales larges et solides, que le *smart contract* ne saurait remplacer en l'état actuel de son développement technologique. Une autre démarche pourrait consister à lister les contrats pour lesquels le recours au *smart contract* serait possible, mais elle serait plus attentatoire à la liberté contractuelle. La deuxième disposition pourrait être celle qui poserait le principe de la séparation entre le contrat, acte juridique conforme au droit qui lui est applicable selon sa nature, sa forme ou son objet, et le *smart contract*, modalité conventionnelle d'exécution du contrat. L'attention des parties qui décideraient de recourir au *smart contract* devrait ensuite être attirée sur la rigueur d'exécution des obligations inhérentes au mécanisme. Dès lors, il semblerait raisonnable que le législateur imposât qu'une information précise fût donnée lors de la conclusion du contrat contenant la clause de recours au *smart contract*. Compte tenu des caractères intrinsèques de la chaîne de blocs et de l'impossibilité de neutraliser l'exécution des obligations enregistrées, et *a fortiori* de les modifier, le Code civil devrait sur ce point rendre obligatoire le versement d'une indemnité compensatrice du préjudice subi par l'exécution d'obligations nulles ou réputées non écrites, que cette compensation ait été prévue dans le *smart contract* ou non. Des dispositions sur la responsabilité devraient également être retenues : responsabilité des créateurs du logiciel si la chaîne de blocs se montre impuissante à réaliser les actions promises (responsabilité, pour faute assurément – pour faute lourde, peut-être), responsabilité des utilisateurs, éventuellement, si l'un d'eux corrompt la chaîne de blocs, privant les parties au contrat de l'exécution automatique de leurs obligations. Il faut toutefois envisager que ces mises en cause soient rendues impossibles par le dispositif décentralisé et anonyme que constitue une chaîne de blocs.

Le *smart contract*, outil de régulation

En matière de contrôle de la concentration économique, l'Autorité de la Concurrence peut subordonner l'autorisation de l'opération à des remèdes qui peuvent prendre la forme d'engagements structurels (cession d'actifs, par exemple) ou comportementaux (suppression d'une clause de non concurrence). Si le respect des engagements structurels est assez facile à vérifier, le contrôle de la bonne exécution des engagements comportementaux est plus délicat à réaliser [12]. L'Autorité de la Concurrence désigne actuellement un mandataire indépendant qui établit des rapports de suivi. Informée des manquements, ladite Autorité peut suspendre ou rétracter la décision d'autorisation, enjoindre sous astreinte aux entreprises d'exécuter ces rapports et infliger une sanction pécuniaire aux entreprises contrevenantes. Le respect de chaque engagement est obligatoire et les sanctions pécuniaires sont établies à un niveau suffisamment élevé pour dissuader les entreprises de les proposer à l'Autorité sans avoir réellement l'intention de les respecter. La mise en place d'une chaîne de blocs privée par l'autorité de régulation permettrait d'automatiser l'exécution des engagements, et peut-être la sanction de leur violation, de manière plus efficace. Mais il faut probablement pour cela que la technologie se perfectionne. La régulation peut l'accompagner ou la suivre, mais en aucun cas la précéder.

(10) http://equationdelaconfiance.fr/rencontre/primavera-de-filippi-il-faut-davantage-enseigner-la-technologie-aux-juristes
(11) Art. 1193 à 1198 actuels du Code civil.
(12) CHEVRIER É., « Du suivi des engagements dans les concentrations », Dalloz Actualité*, 22 septembre 2011.*

Smart contracts… Aspects juridiques !

Par Éric BARBRY
Avocat, directeur du pôle Droit du numérique du Cabinet Alain Bensoussan Avocats Lexing

Les *smart contracts* (traduisez : « contrats intelligents ») ne sont pas une nouvelle forme de contrat qui s'opposerait à des contrats idiots…
À vrai dire, les *smart contracts* ne sont même pas des contrats…
Les *smart contracts* sont une manière de coder un contrat et de rendre son application automatique, donc plus facile, plus rapide et plus sûre.
Les *smart contracts* sont basés sur la technologie de la *blockchain* ». Celle-ci intéresse de très nombreux secteurs d'activité : la finance, la musique, les intermédiaires ou encore les séquestres…
Si, comme toutes les techniques, les *smart contracts* présentent de nombreux avantages, ils posent aussi de nombreuses questions, parmi lesquelles : *quid* de la sécurité ? Qu'en est-il des erreurs de programmation ?

Introduction

Un *smart contract* (littéralement : « contrat intelligent ») n'est pas un contrat : c'est un mode – automatisé et sécurisé – d'exécution d'un contrat.

La question n'est donc pas de rendre un contrat plus « intelligent » ou moins « idiot », mais bien de rendre plus performante sa mise en œuvre.

Cette mise en œuvre, autrement appelée « *contract management* », est aussi importante, sinon davantage, que le contrat en lui-même. En effet, les termes et les dispositions d'un contrat sont importants, mais que sont-ils s'ils ne sont pas (bien) appliqués… ?

Il existe bien des outils de suivi contractuel, mais ceux-ci se résument souvent à assurer le suivi des délais (de renouvellement, par exemple), à faire des relances automatiques sur certains aspects déterminés (la fourniture de documents d'exécution, par exemple) ou encore à suivre des indicateurs (tels que le SLA – *Service-level agreement* – ou le KPI – *Key performance indicator*, par exemple).

Les promoteurs des *smart contracts* nous proposent d'aller un cran, que dis-je, dix crans plus loin.

Utilisant la *blockchain* et « codant » les contrats, les « contrats intelligents » ont pour particularité de s'exécuter automatiquement lorsque sont remplies certaines conditions nécessaires et préalablement déterminées.

Avec le *smart contract*, rien ne change, mais tout est différent.

En effet, rien ne change du côté de la négociation : les parties doivent, dans tous les cas, se mettre d'accord sur quelque chose. Rien ne change non plus s'agissant du contrat lui-même, appréhendé en tant que formalisation de la rencontre d'une offre et de son acceptation.

Cependant, tout est différent en matière d'exécution des termes du contrat, qui ne nécessite plus l'intervention des parties (grâce à leur auto-exécution).

Les *smart contracts* apparaissent comme le nouvel eldorado des juristes technologues que nous sommes.

Pour autant, si les *smart contracts* apportent assurément des avantages, comme toutes les grandes innovations, ils présentent également des faiblesses. Ils intéressent assurément bien du monde, mais leur mise en œuvre nécessite sans doute réflexion.

Les avantages des *smart contracts*

Les *smart contracts* présentent des avantages indéniables pour les juristes.

L'automatisation est une de leurs principales forces, en ce qu'elle conduit mécaniquement à un amoindrissement du risque d'erreur (humaine) dans l'exécution des contrats et, par conséquent, à une diminution des risques ultérieurs de contentieux.

Les *smart contract*s s'exécutant automatiquement, il n'y a plus de risque de ne pas respecter un engagement, et donc de se voir reprocher un *breach of contract* (voire de risquer de « passer à côté » d'un droit).

La *blockchain* n'oublie rien : cette fonction d'exécution automatique permet de mieux gérer les prescriptions contractuelles ou légales.

Les *smart contracts* sont aussi un moyen de « faciliter » l'exécution des contrats. Ces derniers étant par essence numériques, ils peuvent lancer des ordres ou formuler des requêtes tout seuls (comme vérifier la publication de comptes, demander la production de documents, etc.). La *blockchain* peut en effet agir en interaction avec l'ensemble de l'écosystème numérique.

On n'arrête pas une *blockchain* ! De fait, les *smart contracts* permettent de lutter contre les révocations injustifiées. Cette même caractéristique permet de traiter des contrats à multiples acteurs et/ou soumis à de multiples conditions. La *blockchain* en rend la résiliation tout aussi impossible, sauf à entrer strictement dans des catégories prédéterminées et codifiées.

Reposant sur la cryptographie, la *blockchain* permet de garantir l'intégrité des termes d'une transaction. Or, il est primordial, pour les juristes, de pouvoir démontrer avec certitude l'existence même d'un accord et des engagements des parties.

La qualité de « registre » de la *blockchain* permet également à celle-ci d'assurer la traçabilité des actions réalisées, ainsi que les dates auxquelles elles l'ont été. Il n'y a donc plus de discussion sur le fait de savoir si un engagement a été tenu ou non.

La *blockchain* assure également une fonction d'archivage d'une durée quasi indéfinie. Il est courant de perdre un contrat ou des documents d'exécution : tel n'est pas le cas sur la *blockchain*, grâce à laquelle on ne perd jamais rien. Au contraire, on y retrouve tout, et tout le monde y a accès.

À ce propos, la *blockchain* publique assure de manière naturelle une « publicité » aux contrats et aux engagements pris. De fait, elle peut permettre de répondre, là encore par essence, aux obligations de publicité ou de publication de certains actes juridiques.

Au-delà de leurs impacts juridiques, les *smart contracts* sont de véritables *business makers*, car le fait de faciliter l'exécution d'un contrat facilite assurément la vie des affaires. On peut passer plus de temps en avant-vente et moins en *contract management*.

Les faiblesses des *smart contracts*

Reposant sur la *blockchain*, les *smart contracts* embarquent donc avec celle-ci l'ensemble de ses limites et de ses contraintes [1].

Une première critique régulièrement formulée à l'encontre des *smart contracts* est leur propension à augmenter les risques de fraude. À cet égard, nombreux sont les spécialistes qui estiment que la *blockchain* est un environnement ultrasécurisé qui nécessite, pour être forcé, une puissance de calcul tellement considérable qu'il est quasi impossible de la mettre en œuvre.

Ce serait toutefois oublier l'attaque perpétrée en 2016 contre The DAO [2] pour un montant estimé à 50 millions de dollars. Mais la ficelle était un peu trop grosse et les contremesures adoptées (en matière de temps de latence, notamment) ont permis d'éviter le pire. Mais qu'en sera-t-il quand les *smart contracts* seront devenus la norme… ?

Le codage lui-même est un autre point d'attention car, dans tous les cas, il faudra bien recourir à l'humain pour coder le contrat et en paramétrer l'ensemble. Or, cette phase « humaine » est par nature faillible. Le contentieux risque donc de se déporter de l'exécution du contrat lui-même vers la manière dont celui-ci aura été codé et paramétré. Aujourd'hui, en cas de contentieux, les juges lisent le contrat : demain, devront-ils lire des lignes de code ?

Pour les juges, la question de la gestion de la preuve et, d'une manière plus générale, celle de la responsabilité seront à n'en pas douter deux grandes difficultés à résoudre :

- du côté de la preuve, que vaudra une preuve issue de la *blockchain* devant un tribunal ? Les juristes rencontrent déjà les pires difficultés quand il s'agit de produire des *logs* ou des données de connexion : qu'en sera-t-il avec la *blockchain* ?
- du côté de la responsabilité, l'absence de responsable, de gouvernance et donc de « porteur juridique » qui caractérise la *blockchain* constitue également une source de difficultés.

Sur la *blockchain*, tout test est… public. Ceux qui voudraient garder les termes de leur contrat confidentiels devront donc trouver des modèles « privatifs » de *smart contracts*. Sur la *blockchain*, oubliez le droit à l'oubli, et donc la capacité d'effacer les mauvais *deals*.

Le caractère automatique et intègre qui fait la force de la *blockchain* peut également se révéler une faiblesse, notamment quand il s'agit de rompre un contrat de manière anticipée, ou d'en modifier les termes. La notion d'avenant n'est pas des plus compatibles avec les *smart contracts*.

Les *smart contracts*, cas d'usage

Le concept même de *smart contract* ne date pas d'hier. Il a été « inventé » par Nick Szabo qui, dès la fin des années 1990, donnait comme exemple le contrat de location, facile à codifier et prévoyant une restitution immédiate de la propriété d'un véhicule en cas d'impayé.

Il existe bien quelques solutions « opérationnelles [3] », mais elles restent encore confidentielles et pourraient davantage être considérées comme des démonstrations de faisabilité (*Proofs of Concept – PoCs*).

S'il est vrai que tout le monde en parle, peu peuvent se prévaloir d'avoir été confrontés « pour de vrai » aux *smart contracts*. Il est cependant avéré que la *blockchain* intéresse bon nombre de secteurs.

---

(1) « Blockchain, un nouveau champ d'études pour les juristes », Revue Télécom*, n°183, décembre 2016.*
(2) http://www.20minutes.fr/high-tech/1868399-20160618-pirates-derobent-50-millions-dollars-monnaie-virtuelle
(3) www.codius.org ou www.ethereum-france.com ou encore www.slock.it

Sont en premier lieu concernés les secteurs (tels que la banque ou les établissements financiers) dans lesquels il existe de nombreux contrats parfaitement automatisables, dont les caractéristiques sont parfaitement maîtrisées. Le chiffre de 40 milliards de dollars a été avancé comme estimation du coût du suivi des milliards de transactions bancaires [4] effectuées annuellement dans le monde entier.

Les *smart contracts* intéressent également l'ensemble des secteurs ou des acteurs dont l'activité repose sur la mise en place d'un « registre » et induisent une fonction de « notarisation ». Ainsi, à l'instar des autres tiers de confiance, les notaires s'intéressent de près à l'impact des *smart contracts* sur leurs activités.

De la même manière, les *smart contracts* pourraient « disrupter » les fonctions de séquestre, notamment financiers, par le fait que cette fonction pourrait devenir totalement codifiée.

La *blockchain* intéresse également les acteurs dont le cœur de métier (*core business)* repose sur la répartition de redevances financières… À ce titre, elle intéresse assurément la filière musicale, avec l'application du principe selon lequel « si j'écoute tel morceau, alors je paye tel artiste », et sa faculté d'alléger considérablement les frais de gestion [5].

Les *smart contracts* pourraient également « disrupter les disrupteurs ». Un des principaux avantages qu'ils présentent est leur capacité à faire office de « tiers de confiance ». De fait, ils pourraient fort bien sonner le glas des plateformes de mise en relation et d'intermédiation qui ont fleuri sur le *Net* ces cinq dernières années.

Les investissements nécessaires aux études relatives aux *smart contracts* conduisent naturellement la réflexion vers les relations de type *business-to-business* (B2B). Toutefois, les représentants des consommateurs se sont eux aussi intéressés aux atouts que peuvent représenter les *smart contracts* pour les consommateurs.

Ils ont en effet constaté que bon nombre de contrats conféraient des droits aux consommateurs – des droits que ceux-ci « oubliaient » de réclamer ou d'exercer. On peut penser, par exemple, au droit à une indemnité en cas de retard de livraison ou de difficulté de transport (retard de train ou d'avion).

En pratique, les potentiels des *smart contracts* sont innombrables. Prenons l'exemple des paris, secteur dans lequel ils permettraient l'adoption d'une procédure ultra-simplifiée : je parie, je gagne, l'autre paye automatiquement, on le livre, je paye… Rien de plus naturel…

Les *smart contracts* apparaissent donc comme un moyen privilégié de gérer des contrats conclus en nombre : ils permettent d'assujettir les parties à des obligations claires. Ils sont également à privilégier pour les contrats en cascade ou pour les contrats à engagements multiples, dès lors qu'il est possible, grâce à ces contrats intelligents, d'en modéliser la mise en œuvre.

Toutefois, tous les contrats ne sont pas nécessairement « smartisables ».

On peut penser que les contrats de type *business-to-customer* (B2C) seront plus compliqués à mettre en œuvre sous cette forme, nombre de leurs clauses étant « sensibles » et nativement discutables.

Plus complexes également à passer en *smart contracts* seront les contrats dans lesquels la part d'inconnu ou d'imprévu est forte.

Enfin, il est évident que les contrats qui doivent rester confidentiels échapperont à la *blockchain* publique.

Le déploiement des *smart contracts*

Personne ne peut à ce stade prédire si les *smart contracts* auront ou non l'avenir radieux qu'on leur prédit, mais plusieurs questions se posent dès à présent.

La première question est celle des problèmes juridiques faisant obstacle au passage aux *smart contracts*. Aujourd'hui, de nombreux acteurs se lancent dans l'aventure sans même avoir vérifié si le cadre légal, réglementaire ou même jurisprudentiel rendait possible l'usage des *smart contracts*.

La deuxième question porte sur la réalisation de PoC sans la moindre précaution juridique. Or, les *smart contracts* génèrent un certain nombre de problématiques juridiques, à commencer par celles du droit des données à caractère personnel ou de la responsabilité des acteurs impliqués. Il est indispensable de mettre en œuvre ces PoC dans des conditions juridiques maîtrisées (contrat PoC, convention d'expérimentation, expérimentation CNIL si besoin, etc.).

La troisième question porte sur l'opposabilité des *smart contracts* aux juges (notamment de leurs éléments issus de la *blockchain*). Ici, le droit est déjà prêt, en France tout du moins, grâce au droit des « conventions de preuve » [6], qui permettent de définir entre parties contractantes les règles d'opposabilité en termes de preuve. Cependant, ces conventions de preuve devront assurément être conclues avant les *smart contracts* et ne pourront, quant à elles, être codifiées.

À terme se posera également la question de l'opportunité de légiférer ou non en matière de *smart contracts*. À l'instar de la *blockchain* ou des bitcoins, cette question ne manquera pas de se poser.

En France, le législateur est déjà intervenu sur le sujet de la *blockchain*, en termes de mini-bons.

L'introduction de toutes les nouvelles technologies (radio, télé, télécom, Internet, robot…) ayant été accompagnée d'évolutions juridiques majeures, on peut facilement imaginer que le législateur se saisira de la question et qu'il modifiera le Code civil en matière de droit des contrats, comme il l'avait déjà fait en 2000 pour consacrer l'écrit sous forme électronique et en 2004 pour créer une nou-

(4) Voir l'article de Daniel Tourre, www.latribune.fr/opinions/tribunes/blockchain-smart-contract-ou-la-promesse-encore-floue-d-une-revolution-de-la-finance-681096.html
(5) www.alain-bensoussan.com/avocats/technologie-blockchain-avenir-musique/2016/09/23/
(6) Articles 1353 et 1368 du Code civil.

velle catégorie de contrats, en l'occurrence les « contrats sous forme électronique ».

Gageons que, dans ce cas, les dispositions nouvelles « porteront » les *smart contracts* au lieu de les brider.

Épilogue…

Et si les *smart contracts* étaient les pires ennemis des juristes ?

En effet, ils risquent surtout de… « disrupter » les juristes ! Singulièrement ceux du monde du *contract management*.

Ce monde est certes d'ores et déjà bousculé par le nouveau secteur des *LegalTech*, mais les prises de conscience et les capacités d'évolution sont un peu lentes chez nos amis les juristes…

Nombreux sont les secteurs économiques qui se sont lancés dans une réflexion détaillée sur l'impact potentiel des *smart contracts* sur leur profession.

Aussi les juristes, qui sont au cœur même du droit des contrats, seraient-ils bien inspirés d'en faire de même…

La mise en œuvre de la *blockchain* et des *smart contracts* par les industries culturelles

Par Jérôme PONS
Consultant en technologies et stratégies numériques dans les secteurs de la culture et délégué à la normalisation de la *blockchain* chez Music won't stop

La contractualisation est omniprésente dans les industries culturelles, notamment dans les secteurs du cinéma, de la vidéo et de la musique enregistrée. Cependant, les contrats ne sont pas toujours applicables ou exécutés, qu'il s'agisse des contrats d'auteur, d'édition, de licence ou de distribution. Car, en effet, les *minima* garantis peuvent conduire à un transfert « excessif » de la valeur vers les producteurs et les éditeurs, et l'absence de métadonnées juridiques peut pénaliser la rémunération des ayants droit (les artistes-interprètes, par exemple). Dans ce contexte, est-il utopique d'imaginer une programmation et une exécution automatiques des contrats, qui conduiraient à un partage « équitable » de la valeur entre créateurs, producteurs, éditeurs, distributeurs, diffuseurs et consommateurs de contenus numériques et à une rémunération des ayants droit reflétant la consommation au téléchargement ou à l'écoute près ? La technologie *blockchain* répond dans une certaine mesure à cette question.

Les caractéristiques de la *blockchain*

La technologie *blockchain* (littéralement, « chaîne de blocs », que nous avons présentée dans un précédent article : « La *blockchain*, une révolution pour les industries culturelles ? » (http://www.inaglobal.fr/numerique/article/la-blockchain-une-revolution-pour-les-industries-culturelles-9579)) a été imaginée en 2008 par Satoshi Nakamoto à travers sa description du système bitcoin. Ce système de transaction électronique pair-à-pair (P2P) introduit à la fois la crypto-monnaie bitcoin et le réseau P2P de transaction électronique bitcoin (ou réseau bitcoin) [1,2].

Le système bitcoin a été lancé le 3 janvier 2009, date de création du premier bloc de la *blockchain* bitcoin, au sein du réseau bitcoin. Il a été suivi par d'autres systèmes comme Namecoin (crypto-monnaie namecoin), Omni (omnicoin) ou Ethereum (ether), puis complété par des services d'*assets* (s'apparentant à des crypto-monnaies locales, mais dépendant d'un système externe) comme SingularDTV (asset SNGLS basé sur Ethereum) ou MaidSafeCoin (maid, basé sur Omni) (voir la Figure 1 de la page suivante).

Coinmarketcap dénombrait 727 crypto-monnaies et 106 *assets* en circulation au 10 mai 2017.

Dans ce système, chaque transaction est publiée sur le réseau P2P et intégrée à un bloc, puis ce bloc est validé au sein de ce même réseau et ajouté à la *blockchain*.

Une transaction N se caractérise par une empreinte (préfixe 0x suivi de 60 caractères), un horodatage, un montant, des frais, des adresses d'expéditeur A (N) et de destinataire B (N) (préfixe 0x suivi de 40 caractères), un numéro de bloc et par des scripts d'entrée et de sortie.

L'explorateur de blocs Blockchain.info du système bitcoin permet de visualiser une transaction initiée par le service Monegraph et intégrant le *smart contract* lié au dépôt d'une œuvre graphique (voir la Figure 2 de la page suivante).

La troisième ligne des scripts de sortie présente un champ d'informations libres qui autorise de nouveaux domaines d'application de la *blockchain* dans les industries culturelles, notamment la collaboration créative et productive, la désintermédiation dans la distribution des contenus, la gestion de droits, la contractualisation et le paiement électronique. Nous vous proposons, dans cet article, d'approfondir ces applications dans les secteurs du cinéma, de la vidéo et de la musique.

(1) PONS J., « La Blockchain, *une révolution pour les industries culturelles ? », INA Global, 13 mars 2017, www.inaglobal.fr/numerique/article/la-blockchain-une-revolution-pour-les-industries-culturelles-9579*
(2) NAKAMOTO S., "Bitcoin: A Peer-to-Peer Electronic Cash System", 30 octobre 2008, www.bitcoin.org/bitcoin.pdf (version originale) et http://bitcoin.fr/bitcoin-explique-par-son-inventeur/ (traduction française).

Crypto-monnaie (code de la monnaie)	Date de création du premier bloc (bloc de genèse)	Réseau de transaction électronique P2P
bitcoin (BTC ou XBT)	3 janvier 2009	*Bitcoin*
namecoin (NMC)	19 avril 2011	*Namecoin*
litecoin (LTC)	8 octobre 2011	*Litecoin*
nxtcoin (NXT)	24 novembre 2013	*Nxt*
omnicoin (OMC)	4 janvier 2014	*Omni*
dash (DASH)	19 janvier 2014	*Dash*
monero (XMR)	18 avril 2014	*Monero*
xem (XEM)	29 mars 2015	*NEM*
ether (ETH)	30 juillet 2015	*Ethereum*
tao (XTO)	26 août 2016	*Tao*

Asset (code de la monnaie)	Service d'*asset*	Système de transaction électronique P2P
reputation (REP)	*Augur*	*Ethereum*
sngls (SNGLS)	*SingularDTV*	*Ethereum*
maid (MAID)	*MaidSafeCoin*	*Omni*

Figure 1 : Exemples de crypto-monnaies et d'*assets* associés à la technologie *blockchain*.
© Jérôme PONS

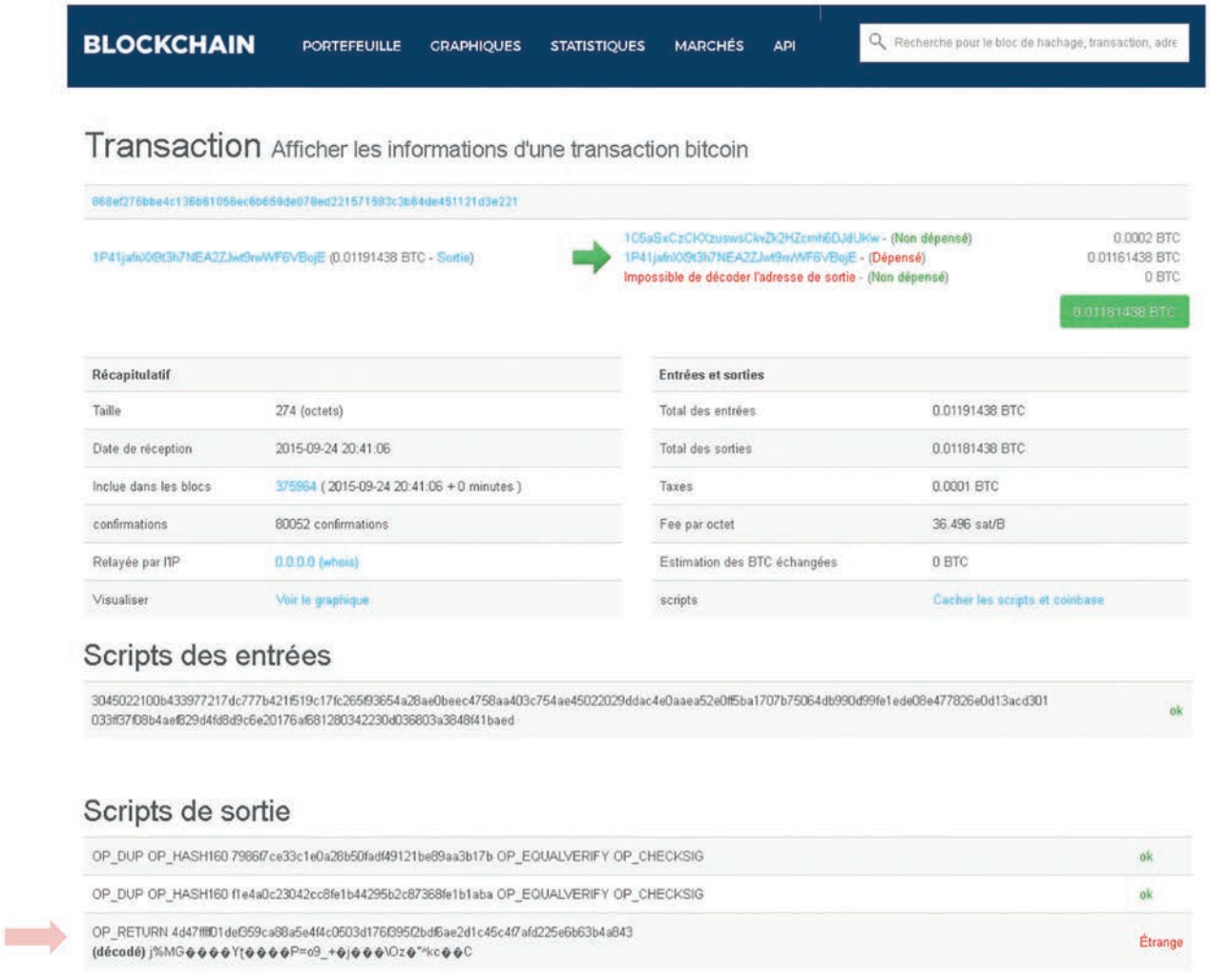


Figure 2 : Visualisation d'une transaction initiée par le service Monegraph.
© Jérôme PONS

Les secteurs du cinéma, de la vidéo et de la musique

Avec la généralisation de la distribution d'œuvres sur Internet, les secteurs de la culture exploitent la même chaîne de transmission convergente des contenus numériques, qui comporte les mêmes étapes de création, de production, d'édition, de distribution, de diffusion et de consommation [3].

Les principales caractéristiques des secteurs du cinéma et de la vidéo

Dans les secteurs du cinéma et de la vidéo, la chronologie des médias séquence l'exploitation du film en salle, sa distribution physique et numérique (de 4 à 48 mois après sa sortie en salle) et sa diffusion à la télévision (de 10 à 30 mois après sa sortie en salle [4]).

Les processus métiers sont organisés en *workflow*, grâce notamment à la norme internationale de cinéma numérique DCI (*Digital Cinema Initiative*). Les différentes étapes de la chaîne de transmission étant chaînées, le passage de relai des données multimédia et des métadonnées d'une étape à la suivante est garanti [5].

Par ailleurs, la contractualisation est rigoureuse, grâce notamment au contrat d'auteur (artiste auteur, comme le réalisateur, le scénariste, le dialoguiste, auteur d'œuvre littéraire), de coproduction, d'artiste-interprète (comédien), d'engagement (technicien comme le chef opérateur ou le monteur, collaborateur comme le scripte, l'ouvrier), de distribution (exploitation) et de diffusion (télévision) ou bien le mandat de distribution (VàD – vidéo à la demande, VàDA – vidéo à la demande par abonnement) et de télévision (voir la Figure 3 ci-dessous).

Il en ressort une certaine transparence des flux financiers liés à des projets de films très subventionnés et à des budgets de production de l'ordre de 1 à 10 millions d'euros, avec un devis moyen des films d'initiative française s'élevant à 5,47 millions d'euros en 2016, d'après le bilan annuel du Centre national du cinéma et de l'image animée (CNC) [6].

De plus, les métadonnées sont consolidées (harmonisées, complétées, fiabilisées), en particulier les métadonnées juridiques utilisées pour la gestion de droits (droit d'auteur) et les métadonnées de contenu utilisées en postproduction (montage) ou en amont de la distribution (affiche du film, copie *Digital Cinema Package* - DCP, DVD). Celles-ci sont renseignées par le scripte, collaborateur artistique et technique du réalisateur, à travers différents rapports (rapport montage, rapport production) [7].

Enfin, en amont de la publication coexistent des bases de données centralisées accessibles. Par exemple, le registre du cinéma et de l'audiovisuel (RCA) du CNC enregistre les contrats associés à la production cinématographique

(3) PONS J., Distribution, partage et stockage des contenus numériques, *Éditions techniques de l'Ingénieur, TI 7536, 10 août 2014, www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/diffusion-distribution-des-images-et-du-son-42507210/distribution-partage-et-stockage-des-contenus-numeriques-te7536/*

(4) Chronologie des médias, CSA, www.csa.fr/Television/Le-suivi-des-programmes/La-diffusion-des-oeuvres/Les-obligations-de-diffusion-d-oeuvres-cinematographiques/Chronologie-des-medias

(5) PONS J., Technologies des contenus numériques : de la production à la protection, *Éditions techniques de l'Ingénieur, TI 7537, 10 août 2015, www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/diffusion-distribution-des-images-et-du-son-42507210/technologies-des-contenus-numeriques-de-la-production-a-la-protection-te7537/*

(6) Bilan 2016 du CNC, CNC, 11 mai 2017, www.cnc.fr/web/fr/bilans/-/ressources/11870403

(7) PANNETIER A., « Le métier de scripte », Commission paritaire nationale Emploi Formation – Audiovisuel (CPNEF-AV), décembre 2010, www.cpnef-av.fr/metiers-realisation/infos/scripte-etude-complete.pdf

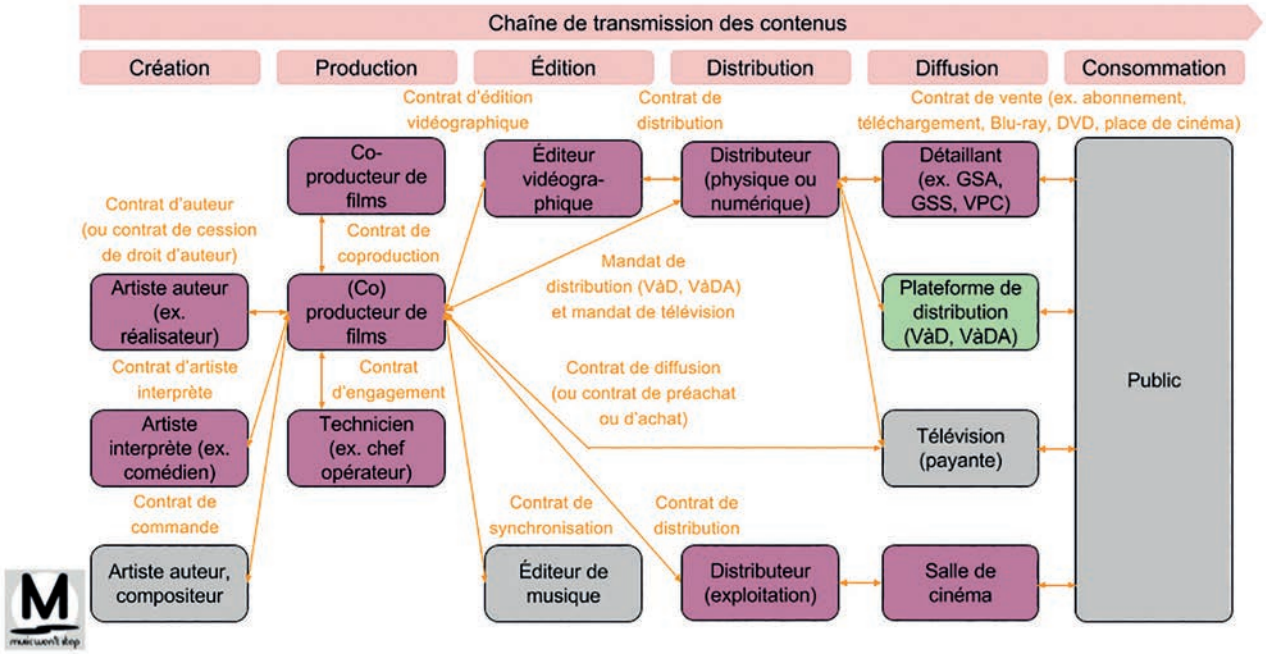


Figure 3 : Exemples de contrats dans les secteurs du cinéma et de la vidéo.
© Jérôme PONS

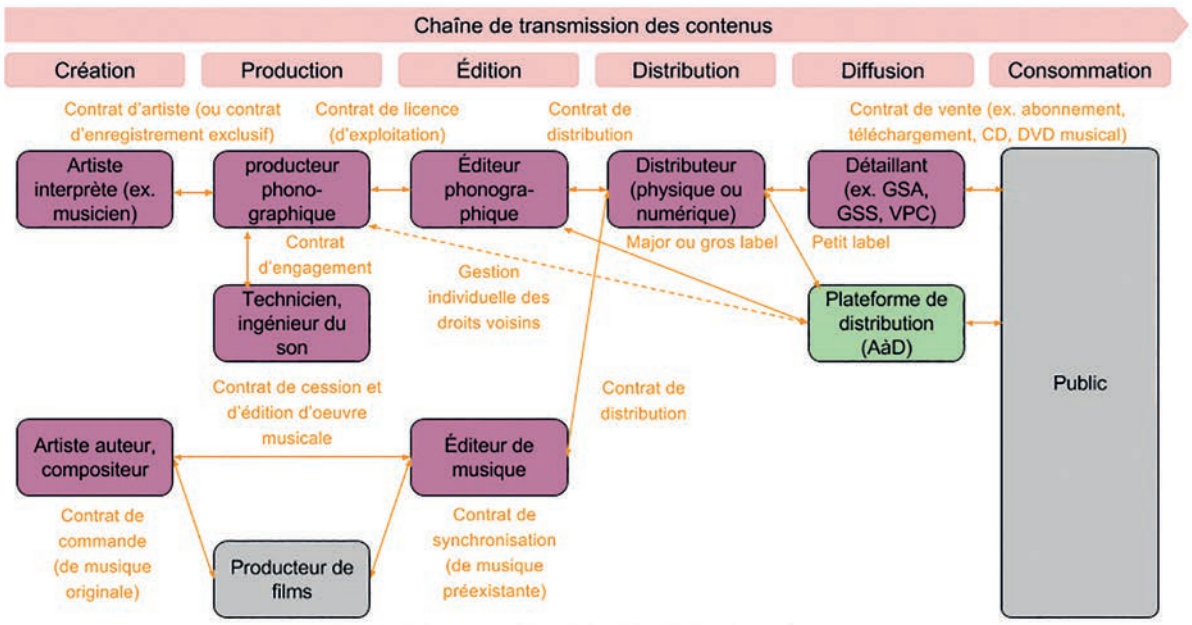


Figure 4 : Exemples de contrats dans le secteur de la musique enregistrée.
© Jérôme PONS

(par exemple, les contrats d'auteur ou de coproduction) et délivre un code d'identification propriétaire (numéro d'immatriculation CNC). La base des visas du CNC enregistre les distributeurs et délivre un numéro de visa. Enfin, la base ISAN (*International Standard Audiovisual Number*) délivre un code d'identification normalisé de l'œuvre audiovisuelle (code ISAN).

De même, en aval de la publication se côtoient des bases de données centralisées accessibles. En particulier, la base IMDb d'Amazon donne accès aux noms des artistes auteurs, comédiens (*casting*) et techniciens présents lors du tournage, au genre du film (comédie, drame…), aux dénominations sociales du distributeur et des coproducteurs, au budget estimé du film (*Box Office*), ainsi qu'aux spécifications techniques du film (par exemple, le modèle de caméra utilisé).

Les principales caractéristiques du secteur de la musique

Dans le secteur de la musique, la simultanéité accompagne chaque publication d'album en termes de distribution physique et numérique, de diffusion à la radio ou à la télévision et de concerts dans le cadre de tournées.

Cette publication s'appuie notamment sur la norme internationale d'échange de données DDEX, qui présuppose que tous les producteurs et éditeurs phonographiques renseignent les métadonnées juridiques et de contenu avant l'étape de la distribution.

De même, la contractualisation est rigoureuse, avec notamment les contrats de cession et d'édition d'œuvre musicale (auteur, compositeur), de commande (de musique originale), d'artiste (artiste-interprète), d'engagement (technicien, ingénieur du son), de licence, de distribution ou de synchronisation (de musique préexistante) (voir la Figure 4 ci-dessus).

L'opacité de certains flux financiers liée à des projets d'albums peu subventionnés et à des budgets de production moins élevés que pour les films (de l'ordre de 10 à 100 milliers d'euros) a été en partie levée dans le cadre de la procédure d'introduction en bourse de Deezer. Nous y avons appris notamment que de 80 à 85 % des *royalties* et des *minima* garantis sont versés aux producteurs-éditeurs phonographiques, tandis que de 10 à 15 % des *royalties* le sont aux sociétés de gestion collective du droit d'auteur [8].

Les métadonnées apparaissent non consolidées, c'est en particulier le cas des métadonnées juridiques utilisées pour la gestion de droits (droit d'auteur, droits voisins), lesquelles gagneraient à être systématiquement renseignées par l'ingénieur du son en marge des sessions d'enregistrement (noms des auteurs, des compositeurs et interprètes et partage des recettes). Il en va de même pour les métadonnées de contenu assemblées à l'étape d'édition (pochette et livret du disque, fichier MP3 *via* le tag ID3) [9].

Pour limiter ce problème, en amont de la publication, se côtoient des bases de données centralisées propriétaires (non accessibles). Par exemple, les bases SCPP (Société civile des producteurs phonographiques), SPPF (Société civile des producteurs de phonogrammes en France), Sacem, Adami (Société civile pour l'administration des droits des artistes et musiciens interprètes) ou Spedidam (Société de perception et de distribution des

(8) PONS J. (auteur principal), « La Révolution numérique, une révolution musicale ! », AFDEL (renommée depuis TECH IN France)/ Forum de Tokyo, 24 novembre 2015, www.forum-tokyo.fr/s/LB_CULTURE_AFDEL_2015_SITE.pdf

(9) PONS J., Les Métadonnées : un enjeu majeur pour le secteur de la musique, *INA Global, 21 avril 2015, www.inaglobal.fr/musique/article/les-metadonnees-un-enjeu-majeur-pour-le-secteur-de-la-musique-8226*

droits des artistes-interprètes) permettent à leurs adhérents de déposer une œuvre musicale ou une musique enregistrée. Les bases IPI de la CISAC (Confédération internationale des sociétés d'auteurs et compositeurs) et IPD de l'IPDA/SCAPR délivrent respectivement des codes d'identification normalisés d'ayants droit (code IPI) et d'artistes-interprètes (code IPN). D'autres bases sont accessibles, comme les bases ISWC de la CISAC et ISRC de l'IFPI, qui donnent respectivement accès aux codes d'identification normalisés d'œuvres musicales (code ISWC) et de musiques enregistrées (code ISRC).

En aval de la publication coexistent des bases de données centralisées propriétaires. En particulier, la base BIPP (Base de données interprofessionnelle des producteurs phonographiques) du SNEP/UPFI/Kantar Media donne accès aux catalogues des producteurs phonographiques actifs sur le marché français, tandis que la base BOEM (Base d'œuvres de l'édition musicale) de la CSDEM/SEAM (Chambre syndicale de l'édition musicale/Société des éditeurs et auteurs de musique) (Paroles CSDEM) fournit les paroles de chansons. D'autres bases sont accessibles, mais elles ne sont pas toujours consolidées, comme le répertoire Sacem, qui associe le code ISWC aux codes IPI (mais pas aux codes ISRC) ou bien la base MusicBrainz, qui relie l'artiste, l'album ou le morceau de musique aux bases externes (par exemple, Discogs, IMDb, Wikidata), à des codes d'identification internes (MBID de MusicBrainz) ou externes (par exemple, code-barres, IPI, ISNI, ASIN d'Amazon, identifiant Discogs), aux plateformes de distribution (comme iTunes, Spotify) et aux empreintes numériques de chaque morceau (AcoustID).

Voyons ci-après quels sont les principaux contrats établis dans ces différents secteurs, et étudions-en le contenu et la modélisation.

Les principaux contrats attachés à ces différents secteurs

Le financement de la culture, la transparence des flux financiers et le partage de la valeur sont régulièrement analysés au travers des contrats, et font l'objet de rapports et de protocoles d'accord.

Les principaux contrats des secteurs du cinéma et de la vidéo

En particulier, le rapport « Chevalier » présente les enjeux du contrat d'association à la production (*via* les SOFICA), le rapport « Bonnell » se focalise sur le contrat d'auteur, tandis que le protocole d'accord « Transparence dans la filière cinématographique » porte sur les contrats d'auteur et d'édition vidéographique. Par ailleurs, le rapport « Gomez » analyse les contrats d'édition vidéographique, de distribution et d'exportation, et le rapport « Lescure » étudie les politiques culturelles de l'ensemble des secteurs de la culture (dont le cinéma, la vidéo et la musique enregistrée). Enfin, le rapport de la Cour des Comptes détaille les contrats d'association à la production, de préachat ou d'achat, de distribution, d'artiste-interprète, ainsi que le mandat de distribution, et propose un « contrat d'objectifs et de moyens [10,11,12,13,14,15] ».

Les principaux contrats du secteur de la musique

De même, le rapport « Zelnik » présente les contrats d'artiste, de licence et de distribution, tandis que les engagements « Hoog » portent sur la publication des conditions générales de vente (CGV), la pérennité et la stabilité des contrats, la justification des avances, la transparence des *minima* garantis, le délai de versement des rémunérations ou les rémunérations versées au bénéfice des artistes-interprètes. En outre, le rapport « Selles » étend l'analyse des contrats précédents aux contrats de cession et d'édition d'œuvres musicales, de synchronisation et d'engagement, et il propose l'adoption du contrat d'association à la production dans le secteur de la musique, ainsi que la mise en place d'un contrat d'objectifs et de moyens. Le rapport « Phéline » se consacre au partage de la valeur et présente les contrats d'artiste et de licence. Enfin, le protocole d'accord « Schwartz » promeut de bonnes pratiques contractuelles par un code des usages et garantit aux artistes une juste rémunération [16,17,18,19,20].

(10) « Rapport Chevalier », CHEVALIER P., « Les SOFICA », rapport remis au CNC, juillet 2008, www.cnc.fr/web/fr/rapports/-/ressources/21531
(11) « Rapport Bonnell », BONNELL R., « Le droit des auteurs dans le domaine cinématographique : coûts, recettes et transparence », rapport remis au CNC, décembre 2008, http://www.cnc.fr/web/fr/rapports/-/ressources/21505
(12) Protocole d'accord « Transparence dans la filière cinématographique », APC/API/ARP/La Guilde (des scénaristes français)/SACD/SCAM/SFAAL/SPI/SCELF/SRF/UPF, 16 décembre 2010, http://guildedesscenaristes.org/uploads/ressbao/accords/protocole_accord_transparence_filiere.pdf
(13) « Rapport Gomez », GOMEZ M., « Mission sur la transparence de la filière cinématographique – La relation entre le producteur et ses mandataires », rapport remis au CNC, septembre 2011, http://www.cnc.fr/web/fr/rapports/-/ressources/622607
(14) « Rapport Lescure », LESCURE M., « Mission Acte II de l'exception culturelle – Contribution aux politiques culturelles à l'ère numérique », rapport remis au ministère de la Culture et de la Communication, mai 2013, www.culturecommunication.gouv.fr/var/culture/storage/culture_mag/rapport_lescure/files/docs/all.pdf (tomes I et II).
(15) Soutien à la production cinématographique et audiovisuelle : des changements nécessaires, rapport de la Cour des Comptes, avril 2014, www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000197.pdf
(16) « Rapport Zelnik », ZELNIK P., TOUBON J. & CERUTTI G., « Création et Internet », rapport remis au ministère de la Culture et de la Communication, janvier 2010, www.ladocumentationfrancaise.fr/var/storage/rapports-publics/104000006.pdf
(17) « Engagements Hoog », HOOG E., « 13 engagements pour la musique en ligne », rapport remis au ministère de la Culture et de la Communication, 17 janvier 2011, Adami/Apple (iTunes)/Beezik/Deezer/ESML/GESTE/MMFF/Orange/Sacem/SCPP/SFA/SNAM/SNEP/Spedidam/SPPF/Starzik/UPFI/VirginMega, www.culturecommunication.gouv.fr/content/download/2292/15440/version/1/file/signature%20accord%20musique%20en%20ligne.pdf
(18) « Rapport Selles », RIESTER F., SELLES D., CHAMFORT A., COLLING D. et THONON M., « Création musicale et diversité à l'ère numérique », rapport remis au ministère de la Culture et de la Communication, septembre 2011, www.ladocumentationfrancaise.fr/var/storage/rapports-publics/114000585.pdf
(19) « Rapport Phéline », PHÉLINE Ch., « Musique en ligne et partage de la valeur – État des lieux, voies de négociation et rôles de la loi », rapport remis au ministère de la Culture et de la Communication, novembre 2013, www.culturecommunication.gouv.fr/Documentation/Rapports/Musique-en-ligne-et-partage-de-la-valeur
(20) « Protocole d'accord Schwartz », SCHWARTZ M., « Pour un développement équitable de la musique en ligne », 2 octobre 2015, CFDT-F3C/ESML/FELIN/GAM/IDOL/MMFF/PRODISS/Qobuz/Sacem/SCPP/SFA/SMA/SNACOPVA CFE-CGC/SNAM-CGT/SNAPS-CFE-CGC/SNEP/SPPF/UPFI, www.culturecommunication.gouv.fr/Presse/Communiques-de-presse/Accord-historique-pour-la-filiere-de-la-musique

Elément constitutif	Sous-élément	Secteur du cinéma et de la vidéo	Secteur de la musique
En-tête	Nature du contrat	Ex. contrat d'auteur (ou contrat de cession de droit d'auteur)	Ex. contrat d'artiste (ou contrat d'enregistrement exclusif)
	Dénominations des parties	Ex. nom et prénom de la personne physique, dénomination sociale de la personnes morale	
	Codes d'identification des parties	Ex. numéro de sécurité sociale de la personne physique, numéro SIRET de la personne morale	
	Qualités des parties	Ex. artiste auteur (réalisateur), producteur de films	Ex. artiste interprète (musicien), producteur phonographique
Clauses contractuelles récurrentes	Objet du contrat	Ex. réalisation d'un film	Ex. fixation d'œuvres musicales
	Durée d'exécution ou période d'exploitation	Ex. durée de la cession	
	Lieu d'exécution ou territoire(s) d'exploitation	Ex. territoires de la cession	
	Mode(s) d'exploitation	Ex. exploitation cinématographique, exploitations secondaires (télédiffusion, vidéogramme) et dérivées	Ex. exploitation phonographique, exploitations secondaires (radiodiffusion, télédiffusion, synchronisation, vidéogramme) et dérivées
Conditions financières	Rémunération	Ex. rémunération proportionnelle (pourcentage calculé sur l'assiette des recettes d'exploitation cinématographique et autres exploitations), rémunération pour droit d'auteur (gestion collective), rémunération pour copie privée (gestion collective), rémunération au forfait	Ex. redevances ou *royalties* (pourcentage calculé sur l'assiette des recettes d'exploitation phonographique et autres exploitations), rémunération équitable et pour copie privée (gestion collective et individuelle)
	Avance sur recettes ou minimum garanti (MG)	Ex. avance (non remboursable) sur la rémunération proportionnelle	Ex. avance récupérable sur les redevances
	Frais		
	Assiette des recettes	Ex. prix public hors taxes (PPHT), recettes nettes part producteur (RNPP)	Ex. prix de gros hors taxes (PGHT) diminué d'un abattement BIEM (exploitation phonographique), prix de gros des vidéogrammes diminué d'un abattement forfaitaire pour conditionnement (exploitation secondaire)
	Modalités de paiement	Ex. règlement par chèque ou virement bancaire	
Conditions générales	Cession de droits	Ex. droit de reproduction et droit de représentation (exploitation cinématographique), droit d'exploitations secondaires (télédiffusion) et dérivées	Ex. droit exclusif de reproduction et de représentation (exploitation phonographique), droit exclusif d'exploitations secondaires et dérivées, droits voisins
	Obligations des parties	Ex. découpage technique du film, choix des artistes interprètes, techniciens et collaborateurs, montage du film par le réalisateur, direction technique et artistique et conservation des éléments ayant servi à la réalisation par le producteur du film	Ex. établissement du programme des séances d'enregistrement par l'artiste interprète, direction technique et artistique et conservation des éléments ayant servi à l'enregistrement du disque par le producteur phonographique
	Publicité et promotion	Ex. crédits (affiche et générique du film)	Ex. promotion du disque par l'artiste interprète, engagement de promotion et de marketing par le producteur phonographique
	Garanties	Ex. garantie des droits cédés par le réalisateur au producteur de films	
	Assurances		
	Registres	Ex. dépôt du contrat au registre RCA du CNC par le producteur de films, obtention du code ISAN par le producteur de films	Ex. obtention du code ISRC de chaque enregistrement par le producteur phonographique
	Clauses spécifiques	Ex. exclusivité de la réalisation, reddition des comptes, droit de préférence	Ex. exclusivité de l'enregistrement, état de redevances, nombre minimum d'enregistrements (albums)
	Modalités de résiliation du contrat	Ex. manquement par l'une des parties à l'une de ses obligations	
	Règlement des litiges et droit applicable	Ex. règlement amiable, recours à un médiateur, recours au tribunal compétent	
En-queue	Date de contractualisation		
	Lieu de contractualisation		
	Nombre d'exemplaires originaux du contrat	Ex. 2 exemplaires	
	Signatures des parties		
Annexes contractuelles	Fixation des prix et recettes	Ex. définition des RNPP (rémunération proportionnelle)	

Figure 5 : Modélisation du contrat traditionnel.

La modélisation du contrat traditionnel

Après analyse, la modélisation du contrat traditionnel nous conduit aux éléments constitutifs suivants (inspirés du rapport Gomez) : en-tête, clauses contractuelles récurrentes, conditions financières, conditions générales, en-queue et annexes contractuelles (voir la Figure 5 ci-contre).

Remarquons que dans le contrat d'artiste, le producteur phonographique ne s'engage à obtenir que les métadonnées juridiques concernant sa rémunération (par exemple, le code ISRC), mais pas celles qui sont nécessaires à la rémunération des auteurs ou de l'éditeur de musique (comme le code ISWC).

Voyons maintenant comment transposer un contrat traditionnel dans un *smart contract*.

La mise en œuvre du *smart contract* par les industries culturelles

Dans un précédent article, nous avions vu à travers la collaboration créative et productive qu'une organisation autonome décentralisée (DAO) était en mesure d'accompagner les créateurs et les producteurs dans leurs processus de création et de production. Pour cela, un *smart contract* (littéralement : « contrat intelligent ») peut être mis en œuvre pour encadrer la description d'une tâche « artistique » (par exemple, écrire une scène d'un scénario ou un couplet d'une chanson, jouer une scène ou un morceau) ou « technique » (par exemple, filmer une scène ou enregistrer un morceau, saisir les métadonnées) ou bien le montant de la rémunération et les droits acquis sur le résultat de la tâche.

Les principes du *smart contract*

L'expression *smart contract* a été définie en 1994 par l'informaticien et cryptographe américain Nick Szabo : « un *smart contract* est un protocole de transaction informatique qui exécute les termes d'un contrat. La conception d'un tel contrat a pour principaux objectifs de satisfaire les conditions contractuelles courantes, de minimiser les exceptions tant malveillantes qu'accidentelles ou le besoin d'intermédiaires de confiance. Les buts économiques associés incluent la réduction des coûts de fraude, d'arbitrage, de mise en application, et autres coûts de transaction [21] ».

Dans le contexte de la *blockchain*, les *smart contracts* constituent juridiquement des « programmes autonomes, codés sur la *blockchain*, qui exécutent automatiquement tout ou partie d'un contrat sans intervention humaine. Dès lors qu'une des conditions préprogrammées du *smart contract* se réalise, la clause contractuelle lui correspondant est automatiquement exécutée » [22].

Par souci de concision, les notions d'identité numérique, de signature électronique, d'oracle ou d'application décentralisée ou distribuée (DApp) ne sont pas développées dans la suite de cet article.

Les trois étapes de la mise en œuvre du *smart contract*

La première étape programme le *smart contract*, de sorte qu'il transpose une ou plusieurs clauses du contrat traditionnel (concernant, par exemple, la rémunération) dans le langage de programmation (langage de script) du système *blockchain*. La seconde étape enregistre le programme informatique associé au *smart contract* dans une *blockchain*. La troisième étape exécute le programme informatique, qu'il s'agisse d'une exécution immédiate de la transaction (comme le paiement électronique) ou d'une exécution déclenchée plus tard par un événement interne au *smart contract* (notamment par la fixation d'une date d'exécution) ou externe (exécution générée par un oracle, tel que défini par le mathématicien et cryptologue anglais Alan Turing) [23].

La mise en œuvre du *smart contract* dans le système Bitcoin

Le langage de script du système Bitcoin, nommé Script, est qualifié d'incomplet au sens de Turing, puisqu'il ne permet pas la création de boucles à l'aide de fonctions récursives.

Ce langage est présenté en piles (*stacks*) dont chacune des lignes comporte une chaîne de caractères ou d'éléments binaires. Les instructions sont traitées séquentiellement jusqu'à la fin du script, sans saut en arrière (absence de boucle). Elles reposent sur plus d'une centaine d'opérateurs de scripts [24] (voir la Figure 6 de la page suivante).

Une transaction est associée soit à un service de paiement électronique, qui utilise des opérateurs de scripts basiques et qui a pour principal objet l'échange de bitcoins entre un émetteur A et un destinataire B, soit à un service « basé sur les scripts », qui utilise des opérateurs de scripts basiques et évolués et qui n'a pas pour seule finalité d'échanger des bitcoins. En particulier, l'opérateur de script évolué OP_RETURN signale un champ d'informations libres contenant les données du *smart contract*.

La mise en œuvre du *smart contract* dans le système Ethereum

Le langage de script du système Ethereum, nommé langage EVM, est qualifié de complet au sens de Turing (*Turing-complete*), puisqu'il autorise les sauts et la création de boucles. Pour éviter qu'une transaction bouclant à l'infini ne bloque le système, l'exécution de la transaction est limitée par la notion de « carburant » (*gas*). Ainsi, lors de la saisie d'un ordre de transaction, le « carburant » est payé à l'avance afin de couvrir le coût d'exécution de la transaction. Une transaction se trouvant « à court de car-

(21) SZABO N., Smart contracts, Best.com, 1994, http://web.archive.org/web/20160323035617/http://szabo.best.vwh.net/smart.contracts.html

(22) VERBIEST Th. (De Gaulle Fleurance & Associés), « Smart contracts *et* blockchain *vont-ils conduire à une révolution juridique ? »,* L'Écho*, 21 avril 2016, http://www.lecho.be/actualite/archive/Smart-contracts-et-blockchain-vont-ils-conduire-a-une-revolution-juridique/9757157*

(23) LAMELA SEIJAS P., THOMPSON S. & McADAMS D., "Scripting smart contracts for distributed ledger technology", Université de Kent au Royaume-Uni/Input|Output Hong Kong, 10 février 2017, http://kar.kent.ac.uk/61162/1/1156.pdf

(24) « Opérateurs de scripts du système Bitcoin » : Script, Bitcoin Wiki, version du 4 mars 2017, http://en.bitcoin.it/wiki/Script

Type d'opérateur	Opérateurs du système *Bitcoin*
Ajout d'une constante à la pile, manipulation de la pile, de la chaîne de caractères, contrôle de flux	OP_i, OP_DUP (duplication de ligne), OP_PICK ou OP_ROLL (copie ou déplacement de ligne en haut de la pile), OP_SIZE, OP_IF, OP_ELSE, OP_RETURN (indique la présence d'un *smart contract*)...
Manipulation d'éléments binaires	OP_EQUAL, OP_EQUALVERIFY...
Opérateur arithmétique	OP_ADD, OP_SUB, OP_MUL ou OP_DIV (addition, soustraction, multiplication ou division)...
Fonction cryptographique	OP_HASH160 ou OP_HASH256 (fonction de hachage générant une empreinte de 160 ou 256 bits), OP_CHECKSIG (vérification de signature)...
Temporisation	OP_CHECKLOCKTIMEVERIFY...

Type d'opérateur	Opérateurs du système *Ethereum*
Manipulation de la pile, de la mémoire, du stockage, contrôle de flux et enregistrement	PUSHi (ajout d'élément), DUPi (duplication d'élément), SWAPi (échange d'éléments), POP (suppression d'élément de la pile), GAS ("jauge de carburant"), JUMP, JUMPI ou JUMPDEST (commandes de saut), LOGi...
Manipulation d'éléments binaires	AND, OR, XOR...
Opérateur arithmétique	STOP (interruption de l'exécution), ADD, MUL, SUB ou DIV (addition, multiplication, soustraction ou division)...
Fonction cryptographique	SHA3 (fonction de hachage générant une empreinte de 256 bits)
Information d'environnement, de bloc	ADDRESS, BALANCE, CODESIZE, GASPRICE ("prix du carburant"), BLOCKHASH, TIMESTAMP, NUMBER...
Opérateur système	CREATE (création d'un nouveau compte), CALL (envoi d'un message à un compte), RETURN, SUICIDE (destruction d'un compte)...

Figure 6 : Exemples d'opérateurs de scripts utilisés par les systèmes Bitcoin et Ethereum.
© Jérôme PONS

burant » est annulée, prévenant ainsi le risque de générer d'éventuelles boucles à l'infini.

Ce langage est exécuté par la machine virtuelle Ethereum (EVM - *Ethereum Virtual Machine*) et est présenté en piles, sous la forme de chaînes de caractères. Les instructions sont traitées séquentiellement, permettent le saut en arrière (présence de boucles) et s'appuient sur plus d'une centaine d'opérateurs de scripts [25].

Une transaction est associée nativement à un service « basé sur les scripts », appelé *smart contract*, utilisant des opérateurs de scripts basiques et évolués et échangeant des ethers (le paiement électronique est un usage parmi d'autres du *smart contract*).

(25) « Opérateurs de scripts du système Ethereum », WOOD Gavin, "Ethereum: A Secure Decentralised Generalised transaction Ledger, Ethereum/Ethcore", révision EIP-150, http://gavwood.com/Paper.pdf

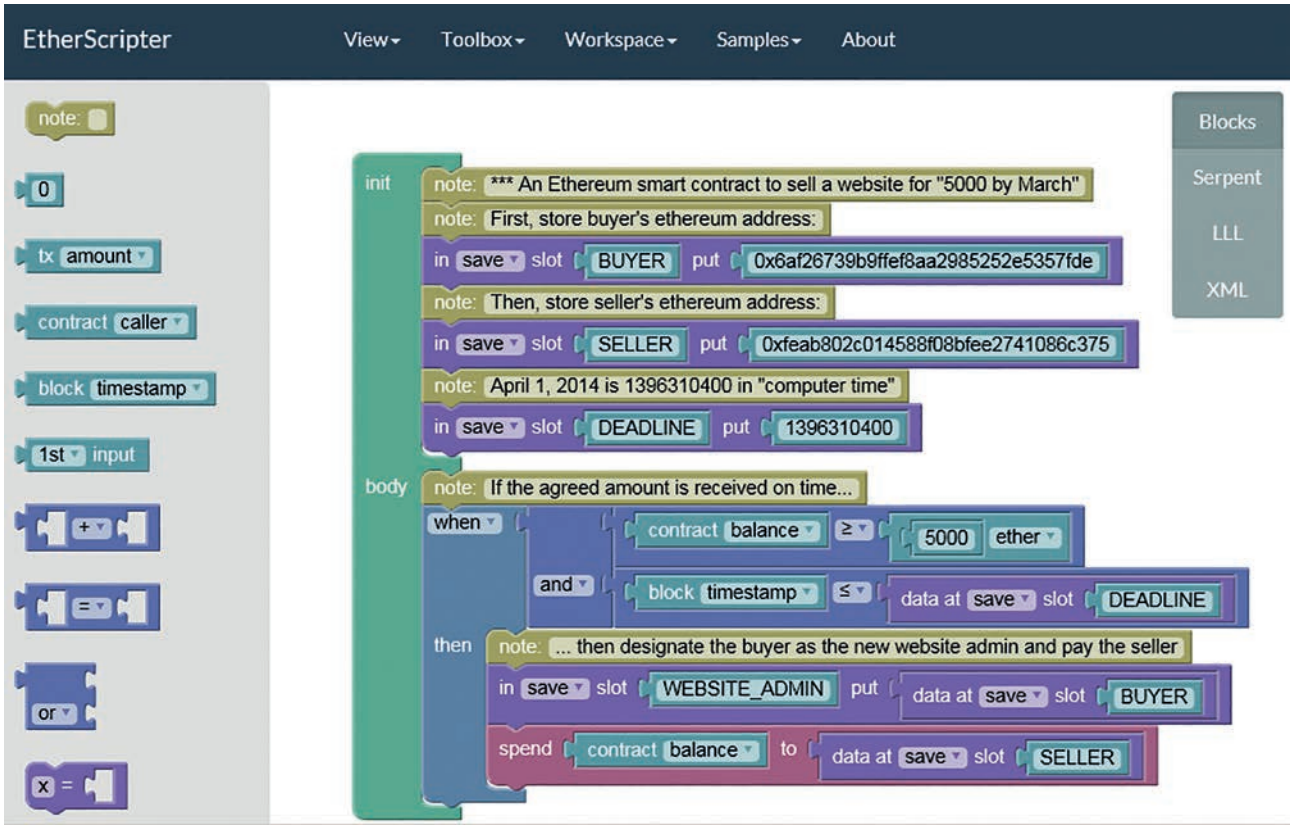


Figure 7 : Transposition de certaines clauses du contrat traditionnel en langage de *script* de haut niveau avec EtherScripter.

Ce *smart contract* est vu comme une entité virtuelle disposant de son propre code de script capable d'émettre et de recevoir des messages et des ethers, de créer d'autres contrats ou de s'autodétruire. Il ne peut pas initier de transaction, mais il peut être activé par une autre transaction lui étant destinée [26].

En plus du langage EVM, un langage de script de haut niveau peut être utilisé comme Solidity, Serpent ou LLL. Dans la pratique, un éditeur comme EtherScripter permet de transposer certaines clauses du contrat traditionnel (par exemple, contrat de vente), qu'il traduit alors en langages de script de haut niveau tels que Serpent ou LLL (voir la Figure 7 de la page précédente).

Un cas d'usage, l'expérimentation Ujo Music

Lors de l'ouverture du service Ujo Music en version alpha (le 2 octobre 2015), seul le morceau Tiny Human de l'artiste anglaise Imogen Heap était disponible. Notons que ni l'œuvre musicale ni l'enregistrement associés à ce morceau ne sont inscrits dans les bases ISWC et ISRC. En revanche, l'artiste est identifiée par le code ISNI 0000000078404022 et créditée, d'après le service, comme auteure, compositrice, arrangeuse, interprète et productrice du morceau.

Cinq modes de distribution du morceau étaient proposés, dont le téléchargement au prix de vente de 0,6 dollar et le *streaming* à 0,006 dollar par écoute. Les conditions générales de vente indiquent que le partage des recettes était de 91,25 % pour Imogen Heap et de 1,25 % pour chacun des six musiciens et pour l'ingénieur du son.

L'achat et le téléchargement du morceau mettaient en œuvre un *smart contract* dans le système Ethereum. Le service Ujo Music s'interconnectait à la plateforme d'échange Kraken afin d'indiquer le taux de conversion du prix de vente (par exemple, 0,6 dollar = 0,48 ether) et pour permettre à l'acheteur de créer un portefeuille électronique, d'obtenir une adresse de compte, d'alimenter son compte (par exemple, 1 ether) et de saisir l'ordre de transaction à destination de l'adresse fournie par le service Ujo Music [27].

Par ailleurs, le service Ujo Music fournissait en toute transparence la liste des transactions associées au morceau (voir la Figure 8 ci-dessous).

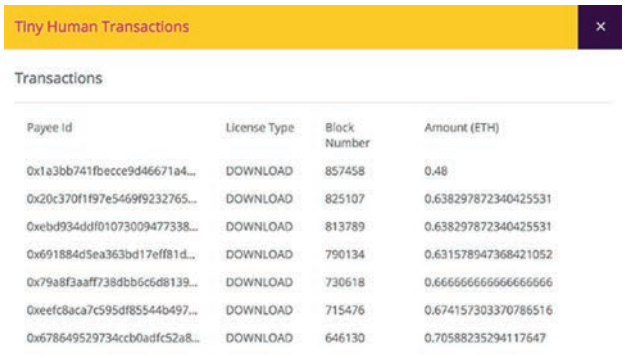


Figure 8 : Liste des transactions associées au morceau Tiny Human.

L'explorateur de blocs Etherscan du système Ethereum permet de retrouver le numéro de bloc 857458 et de visualiser la transaction de 0,48 ether initiée par le service Ujo Music, intégrant le *smart contract* lié au téléchargement du morceau (voir la Figure 9 ci-dessous).

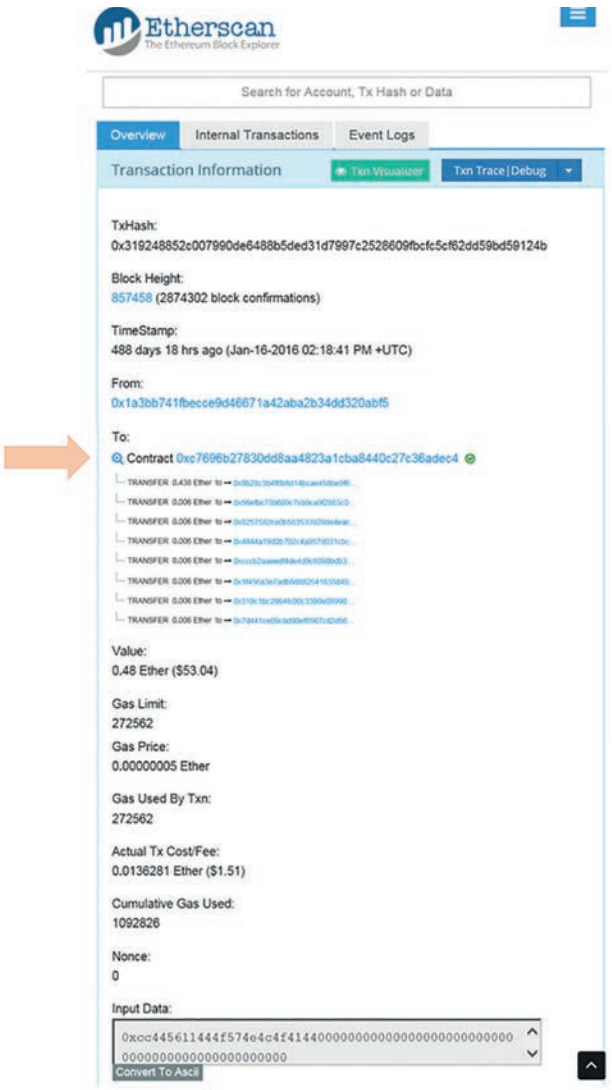


Figure 9 : Visualisation d'une transaction initiée par le service Ujo Music.

Identifiée par son empreinte, la transaction comporte un horodatage (16 janvier 2016 à 14h 18m 41s), elle mentionne la présence d'un *smart contract*, un « prix du carburant » et des frais de transaction. L'exécution immédiate du *smart contract* a réparti le montant de la transaction (0,48 ether) vers l'adresse d'Imogen Heap (0,438 ether) et vers chacune des 7 autres adresses (0,006 ether), ce qui

(26) BUTERIN V., "Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform", Bitcoin Magazine/ Ethereum, *23 janvier 2014, http://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/*

(27) "Part 1: How we tried to buy Imogen Heap's song on Ethereum", Hatching Amazing, *24 janvier 2016 http://medium.com/hatching-amazing/part-1-how-my-ssn-prevented-me-from-buying-music-on-the-blockchain-and-why-blockchain-for-music-a85eaea-ca7ad*

correspond bien au partage des recettes indiqué dans les CGV.

Les perspectives des *smart contracts* pour les industries culturelles

Lorsque la technologie *blockchain* est exploitée pour mettre en œuvre des *smart contracts* dans les secteurs de la culture, cela implique nécessairement un dialogue entre des informaticiens, des juristes et des acteurs de la chaîne de transmission des contenus numériques.

Face à un cas d'usage, ceux-ci doivent d'abord adopter une crypto-monnaie (par exemple, Bitcoin, Ethereum, Omni) ou un *asset*, ce qui les orientera vers un système *blockchain*. Ensuite, ils doivent transposer une ou plusieurs clauses du contrat traditionnel dans le langage de script de ce système, pour, enfin, s'assurer, à l'aide d'un explorateur de blocs, que le *smart contract* est effectivement exécuté.

La *blockchain* apporte des solutions à des problèmes connus, comme le rapprochement des codes ISRC et ISWC (dans le secteur de la musique enregistrée). À cet effet, trois sociétés de gestion collective du droit d'auteur (ASCAP aux États-Unis, PRS for Music au Royaume-Uni et la Sacem en France) se sont alliées à IBM, en avril 2017, afin de rapprocher ces codes en s'appuyant sur le projet *Hyperledger Fabric*. Des *smart contracts* automatisant l'attribution de couples (ISRC, ISWC) et simplifiant la gestion des droits pourraient alors émerger [28].

Les codes d'identification utilisés par les industries culturelles (par exemple, ISAN, ISRC, ISWC) ont été normalisés par l'Organisation internationale de normalisation (ISO), qui a d'ailleurs créé en 2016 le Comité technique ISO/TC 307 consacré à la *blockchain* et aux technologies de registre distribué (DLT). Comptant 19 pays participants (dont la France, représentée par l'AFNOR), ce comité s'est réuni pour la première fois en avril 2017. Il a voté la création d'un groupe d'étude dédié aux *smart contracts* (ISO/TC 307/SG5) qui devra « considérer l'application de méthodes de programmation et de langages de script permettant à des non-informaticiens d'exprimer des clauses contractuelles [29] ».

Dans le contexte de la *blockchain*, le secteur de la musique se trouve encore une fois aux avant-postes de la transformation numérique. Il pourrait se voir emboîter le pas par les secteurs du cinéma et de la vidéo, d'autant plus que les travaux de normalisation internationale des *smart contracts* apporteront davantage de limpidité.

(28) « Blockchain : la Sacem, Ascap et PRS for Music s'allient pour une meilleure identification des œuvres », Sacem, communiqué de presse du 7 avril 2017, http://societe.sacem.fr/actualites/innovation/blockchain--la-sacem-ascap-et-prs-for-music-sallient-pour-une-meilleure-identification-des-oeuvres

(29) « ISO/TC 307 Chaîne de blocs et technologies de registre distribué électronique », ISO, www.iso.org/fr/committee/6266604.html

Acronymes

AàD : Audio à la Demande

AFNOR : Association française de normalisation

ASIN : *Amazon Standard Identification Number*

CGV : Conditions Générales de Vente

CNC : Centre national du cinéma, de l'image et du son

DAO : *Decentralized Autonomous Organization*

DCI : *Digital Cinema Initiative*

DCP : *Digital Cinema Package*

DDEX : *Digital Data Exchange*

DLT : *Distributed Ledger Technology*

EVM : *Ethereum Virtual Machine*

GSA : Grande Surface Alimentaire

GSS : Grande Surface Spécialisée

IPD : *International Performers Database*

IPI : *Interested Parties Information*

IPN : *International Performer Number*

ISAN : *International Standard Audiovisual Number*

ISO : *International Standards Organization*

ISRC : *International Standard Recording Code*

ISWC : *International Standard Musical Work Code*

LLL : *Lisp Like Language*

MBID : *MusicBrainz IDentifier*

MG : Minimum Garanti

P2P : *Peer-to-Peer*

PGHT : Prix de Gros Hors Taxes

PPHT : Prix Public Hors Taxes

RCA : Registre du Cinéma et de l'Audiovisuel du CNC

RNPP : Recettes Nettes Part Producteur

SOFICA : Société de financement de l'industrie cinématographique et de l'audiovisuel

VàD (A) : Vidéo à la Demande (avec Abonnement)

VPC : Vente Par Correspondance

L'Oracle *hardware* : la couche de confiance entre les *blockchains* et le monde physique

Par Vanessa RABESANDRATANA
Customer Success Manager, Ledger
et Nicolas BACCA
Chief Technical Officer, Ledger

Les applications *blockchain* évoluent dans leur propre environnement entièrement virtuel qui est par construction complètement séparé du monde réel. Les *smart contracts*, applications décentralisées et autres crypto-monnaies ont donc une emprise limitée sur le monde concret qui nous entoure. On peut même parler d'orthogonalité : ces deux univers existent sur des plans qui ne se superposent jamais.
Chaque cas d'usage nous renvoie alors à cette problématique : comment les applications liées à la *blockchain* peuvent-elles interagir de façon efficace et sécurisée avec le monde réel, et comment les *smart contracts* peuvent-ils se nourrir de données externes, le tout, de façon sécurisée et efficace ?
Cette question s'est posée tout naturellement dès les balbutiements de cette technologie et il a fallu concevoir des outils et des interfaces adaptés. La plateforme de confiance qui permet de tisser des liens entre le monde réel et la *blockchain* porte un nom : Oracle.

Les Oracles sont des entités de confiance qui signent (et attestent) des revendications concernant l'état du monde.

En fonction de ce que nous appelons de manière exacte le « monde physique », et de l'existence ou non d'un consensus sur l'état de ce que nous devons évaluer, il existe différentes implémentations possibles d'Oracles.

Les Oracles logiciels

Les Oracles fondés sur l'attestation d'origine

Lorsque la connaissance de l'information recherchée est disponible en ligne, des Oracles basés sur des implémentations logicielles peuvent fournir des solutions efficaces. Ils répondent à des questions simples telles que : « Quelle est la valeur d'un bitcoin en euros ? » ; « Est-ce que cet avion a connu un retard de plus de 30 minutes ? » ou encore « Est-ce qu'il pleuvait hier, dans cette ville ? ». Les données sont disponibles en ligne, sur Internet, et peuvent être extraites de sources fiables telles que des compagnies aériennes, des agrégateurs de données financières ou des instituts météorologiques.

L'Oracle peut attester cryptographiquement de l'origine des données (en vérifiant la source de l'information, elle-même signée par un certificat TLS) et pousser l'information vers un *smart contract*. En quelque sorte, ce type d'Oracle fait une déclaration publique et vérifiée sur la véridicité du contenu de pages *Web* sécurisées, tout en fournissant une passerelle utilisable par des applications décentralisées.

Si cette approche est plutôt simple à mettre en œuvre, elle pose un problème de taille : vous devez non seulement faire confiance à l'Oracle sur le fait qu'il ne va pas déformer l'information, mais vous devez surtout faire confiance à la source elle-même ! Pour les données météorologiques provenant d'un site *Web* réputé, cela peut aller de soi. Mais qu'en est-il de questions plus complexes, de faits ou d'événements pas toujours faciles à exprimer ? Devrions-nous, par exemple, avoir une confiance aveugle en Wikipédia ? Les controverses entre ses différentes versions pourraient sérieusement mettre à mal l'Oracle et, au final, ses affirmations seraient sans valeur.

Les événements très concrets peuvent toujours être vérifiés à partir de différentes sources de confiance (index financiers, données météorologiques, résultats sportifs...), mais cela ne fonctionnera pas pour des questions plus complexes qui peuvent donner lieu à des vérités différentes en fonction de qui les observe ou de qui a un intérêt à en présenter une version biaisée.

Les Oracles fondés sur le consensus

Les marchés prédictifs sont d'excellents exemples d'applications décentralisées qui ne peuvent exister en l'absence d'Oracles « parfaits ». Le principe est de pouvoir parier sur des événements, quels qu'ils soient, et de pouvoir déduire des enjeux des tendances fortes, et donc d'avoir une vision de l'avenir. Si l'on pense immédiatement aux paris sportifs ou aux dérivés financiers et aux *futures*, les marchés prédictifs peuvent aussi apporter des informations critiques dans le domaine du renseignement, des opérations militaires ou de la lutte contre le terrorisme. Si quelqu'un avait des informations valables sur un fait majeur et s'il pouvait les monétiser de façon sécurisée et anonyme, alors celles-ci finiraient par être exposées sur le marché prédictif.

L'accès à certaines informations étant un monopole d'État et la réglementation ne permettant pas l'opération de tels marchés prédictifs, l'approche décentralisée est aujourd'hui la seule solution. L'Oracle, qui détermine au final la vérité d'un fait pour solder les paris, doit donc lui aussi être décentralisé et de toute confiance. Comme il est impossible de se baser sur une source unique (celle-ci étant trop facilement manipulable ou censurable), il est nécessaire de faire appel à la sagesse de la foule et d'utiliser des mécanismes de consensus plutôt complexes basés sur la réputation et sur la nécessité d'enjeux pour « punir » ceux qui ne respecteraient pas l'obligation de vérité.

Ces Oracles décentralisés font l'objet aujourd'hui d'une R&D active dans le cadre de marchés prédictifs tels qu'Augur ou Gnosis. Mais il reste encore à démontrer que le système pourra fonctionner de façon « parfaite », seule possibilité pour qu'il ait la moindre valeur.

Les Oracles *hardware*

Si nous avons vu que les Oracles permettent de traiter les événements que l'on pourrait qualifier de publics et d'observables par tous, qu'en est-il des événements en temps réel, privés et centrés sur un utilisateur ou sur un objet en particulier ?

Il existe des faits qui ne peuvent être déterminés par consensus ou par attestation de données publiques. Nous pourrions, par exemple, citer les questions suivantes :

- « Où est ce conteneur, maintenant ? »
- « Est-ce que cette porte est verrouillée ? »
- « Quelle est la vitesse actuelle de ce véhicule ? »
- « Combien ai-je fait de pas aujourd'hui ? ».

Sources de données locales et privées

Certaines applications nécessitent d'obtenir des informations liées à des événements physiques dont les données n'existent que dans l'objet ciblé (ou dans la personne ciblée). La mesure doit être effectuée localement, souvent en temps réel. Comme les données sont privées, la précision de l'information ne peut être vérifiée ni par un flux public ni par consensus.

On peut imaginer de nombreux cas d'usage :

- l'économie collaborative,
- la traçabilité industrielle,
- les *smart grids*,
- ...

Prenons l'exemple d'une assurance automobile *smart contract* dont les conducteurs paieraient une prime dans l'espoir d'être récompensés pour leur bon comportement sur la route. Les conducteurs coupables d'excès de vitesse perdraient leur prime, qui serait reversée dans un pot commun partagé au final entre tous les « citoyens respectueux de la loi ». Les associations de sécurité routière pourraient contribuer localement *via* l'octroi de primes supplémentaires à inciter plus encore à une bonne conduite.

La difficulté dans cette approche est de trouver un moyen sécurisé et infalsifiable permettant de surveiller la vitesse des véhicules : si l'on pouvait soit simuler une conduite parfaite soit attacher le *tracker* à une autre voiture, le système d'assurance deviendrait totalement inutilisable et finirait par péricliter.

Les capteurs sécurisés par attestation cryptographique

Si l'on souhaite pouvoir effectuer une mesure de façon totalement sécurisée en ayant la garantie de son origine, il est nécessaire de mettre en place les éléments suivants :

- une attestation cryptographique du capteur créant une authentification de l'origine de la lecture : un élément sécurisé effectue l'orchestration de la carte électronique et signe les paquets de données sortants (avec un nonce, pour éviter les répétitions) ;
- une installation anti-falsification du dispositif de mesure, le rendant immédiatement inopérant *via* l'effacement des clés privées en cas de tentative de manipulation (connexion à un autre objet, injection de faux stimuli, etc.).

Ces dispositifs de lecture sécurisés portent le nom d'*Oracle hardwares* : ils jouent le rôle de passerelles permettant de passer du monde physique à l'espace virtuel *blockchain*.

Le déploiement de ces Oracles nécessite la mise en place de provisionnements (clés d'attestation et clés d'identification de l'appareil), ainsi que l'établissement d'une stratégie de supervision d'installation (permettant de s'assurer que les capteurs mesurent bien ce que l'on souhaite mesurer). La confiance à long terme est garantie par l'anti-falsification et la protection des clés privées grâce à l'usage d'éléments sécurisés.

Dans le cas de l'exemple de l'assurance auto précédemment évoqué, l'Oracle doit avoir les clés d'attestation appropriées (ce qui implique qu'il se soit approvisionné auprès de fournisseurs spécifiques) et une stratégie d'audit doit être mise au point afin de vérifier que la mise en place initiale est correcte (cela nécessitant des parties/vérificateurs externes).

Vers une généralisation des Oracles ?

Pour multiplier les cas d'usage, les applications décentralisées ne peuvent échapper à la nécessité de puiser des informations dans l'univers physique qui nous entoure.

La notion d'Oracle devient donc essentielle. Elle se positionne au cœur des éléments indispensables au développement de ces technologies.

Aujourd'hui, les industriels ont tout intérêt à anticiper sur l'évolution de ces nouveaux modèles et à intégrer dans leurs équipements les fonctionnalités d'Oracle *hardware*. On peut donc imaginer qu'il y aura, dans un futur proche, des compteurs intelligents dialoguant nativement avec des *blockchains* ou avec des véhicules électriques intégrant des portefeuilles cryptographiques permettant un paiement machine-à-machine.

L'Internet des objets devra donc aussi compter avec les technologies *blockchain*, celles-ci étant de nature à faciliter l'intégration d'éléments de sécurisation qui font aujourd'hui grandement défaut dans ce nouvel univers désormais si proche.

Pourquoi la normalisation s'intéresse-t-elle à la *blockchain* ?

Par Olivier PEYRAT
Directeur général de l'Association française de normalisation (Afnor)
et Jean-François LEGENDRE
Responsable développement Afnor

La *blockchain* concerne un ensemble de technologies. Son potentiel de développement est considérable, avec de nombreux cas d'usage envisagés, dont certains sont déjà en phase de déploiement. L'impact potentiel de la *blockchain* est disruptif, et sans doute stratégique pour de nombreux secteurs. Toutefois, la *blockchain* devra atteindre un premier niveau de maturité, ce qui implique le développement de normes afin d'apporter la confiance nécessaire sur certains aspects des processus mis en œuvre.

Introduction

Avec la transformation numérique de la société, de nombreux acteurs expriment un besoin de traçabilité sous la forme de l'enregistrement de transactions variées, non nécessairement financières. Cette traçabilité est nécessaire pour l'établissement et l'utilisation de services de confiance. Elle constitue, en quelque sorte, une transposition de principes respectés par de nombreux services de l'économie avant leur entrée dans l'ère digitale.

Nées il y a une dizaine d'années [(1)] en tant que support technique à la monnaie virtuelle bitcoin, les technologies de notarisation distribuées, appelées *blockchains,* suscitent un vif intérêt depuis quelques mois, et ce, pour partie grâce à l'accélération de la transformation numérique de la société et des entreprises. Le sujet *blockchain* figure ainsi au sommet du pic d'inflation de la courbe d'Hype de maturité des technologies ! Aussi la liste des cas d'usage potentiels augmente-t-elle de jour en jour : secteur financier (dont les assurances), industrie du médicament, énergie, agroalimentaire, gestion de droits de propriété intellectuelle, gestion de cadastres ou d'héritages, etc.

La promesse de la *blockchain* est d'offrir un système sûr, robuste, ouvert et public de notarisation d'enregistrements sans recourir à aucun tiers de confiance centralisé.

Qu'est-ce qu'un système de notarisation distribué ?

Il s'agit d'un système décentralisé d'enregistrement de l'historique exhaustif de toutes les « transactions » effectuées depuis sa création. On parle ainsi d'un grand livre de comptes, par analogie avec la pratique ancestrale des entreprises pour tracer leurs entrées et leurs dépenses. Dans un tel système, les transactions sont consignées dans le « grand livre de comptes » par blocs consécutifs, chaque bloc réunissant un ensemble de transactions ayant été validées, condition nécessaire pour que le bloc soit ajouté à la chaîne.

Ce qui caractérise de façon fondamentale ce système d'enregistrement décentralisé, c'est le fait que ce livre de comptes est partagé et mis à jour de façon distribuée, au sein d'un réseau. Chaque nœud du réseau possède ainsi sa propre copie actualisée en permanence du « grand livre de comptes ». Différents mécanismes, que l'on n'expliquera pas ici, permettent d'assurer la sécurité du dispositif. On en retiendra les caractéristiques suivantes, qui ont un impact certain sur le cahier des charges des normes et standards susceptibles d'être développés à cet effet :

- le respect de l'anonymat, entre l'émetteur et le récepteur d'une transaction, grâce à des techniques de multi-signatures digitales ;
- la minimisation de la connaissance que doit posséder chaque nœud pour pouvoir calculer la validité d'une transaction ;
- une écriture comptable partagée par les nœuds du réseau et fondée sur une méthode de « consensus » de la majorité des nœuds de réseau pour pouvoir valider une transaction ;
- une transparence totale du « grand livre de comptes » et des transactions effectuées ;
- dans le cas d'usage Bitcoin, un modèle économique spécifique pour rémunérer les nœuds de réseau qui vérifient les transactions.

(1) En 2008, un développeur (ou un collectif ?), se faisant appeler Satoshi Nakamoto, publie sous licence libre MIT le protocole de la blockchain *dans un logiciel écrit en C++. Un an après, la première plateforme de crypto-monnaie basée sur l'implémentation de ce protocole était lancée, sous l'appellation de bitcoin.*

Photo © Jens Kalaene/Picture alliance-ZB-MAXPPP

Possibilité offerte d'un paiement en bitcoins sur un site de commerce électronique.

« La première application de la *blockchain* a été la monnaie virtuelle bitcoin ».

Photo © Romanpoet Wikimedia

Portrait de Vitalik Buterin (Wikimedia Commons).

« En 2013, un étudiant du nom de Vitalik Buterin eut l'idée de créer un protocole *blockchain* qui intégrerait un langage de programmation complet afin que l'on puisse écrire dans la *blockchain* les règles de n'importe quelle application. »

Le terme de « transaction » est à entendre au sens large. En effet, la première application de la *blockchain* a été la monnaie virtuelle bitcoin. Très vite, il a été envisagé d'utiliser la *blockchain* pour tout autre chose. En 2013, un étudiant du nom de Vitalik Buterin eut l'idée de créer un protocole *blockchain* qui intégrerait un langage de programmation complet afin que l'on puisse écrire dans la *blockchain* les règles de n'importe quelle application. Après l'une des plus importantes levées de fonds participatives de l'histoire des nouvelles technologies, c'est sur ce principe que la plateforme Ethereum a été mise en service, en 2015.

Avec cette notion de « contrats intelligents », qui sont en fait des éléments exécutables de logiciels, il devient possible de mettre en œuvre un système dynamique permettant d'inscrire et de tracer dans le « grand livre de comptes » toutes sortes d'actes « intelligents » à sécuriser – tels qu'un diplôme, qui sera validé de façon conditionnelle, une élection, un cadastre ou une émission de titres, par exemple –, et d'intégrer dans les blocs de la chaîne des actions à réaliser automatiquement lorsque les conditions de production d'un résultat sont remplies, par exemple déclencher le versement d'un héritage après un décès.

Ce système permet donc à chaque acteur de connaître potentiellement tout ce qu'il se produit dans le monde digital, d'enregistrer le fait que l'événement a eu lieu, le cas échéant qu'il s'est déroulé correctement, de déclencher des actes associés – le tout, naturellement, sans exposer des détails confidentiels à propos du sujet ou des parties prenantes impliquées.

Les enjeux de la normalisation volontaire

Les normes sont des documents d'application volontaire établies par un organisme de normalisation reconnu comme respectant des principes de pluralité de la représentation des parties intéressées, d'ouverture et de transparence en matière de gestion des droits de propriété intellectuelle.

De prime abord, le protocole *blockchain* est un ensemble de technologies « ouvertes », c'est-à-dire publiées en source libre suivant une licence ouverte et largement documentée [2]. Les fonctions de sécurité utilisées sont elles-mêmes bien connues (*hash*, signature digitale, etc.). Tout cela, *a priori*, ne requiert pas d'action particulière au niveau de la normalisation internationale !

Ce point de vue devra cependant considérablement évoluer si l'on souhaite que ces technologies entrent rapidement et à juste titre dans une phase de maturité.

Un premier risque est en effet constitué par la multiplication des implémentations du protocole *blockchain* : même si l'on se limite aux seules crypto-monnaies, il s'agit d'un protocole de réseau qui, aujourd'hui, régit plusieurs centaines de plateformes à des stades plus ou moins avancés de déploiement, dont la plus connue est évidemment la plateforme historique bitcoin. Cette multiplication représente en soi un sujet de préoccupation pour les utilisateurs, car on ne peut se satisfaire d'une standardisation de fait qui s'effectue aujourd'hui au travers d'une API (Interface programmatique) spécifique à chaque plateforme (Bitcoin, Ethereum, Nxt…).

Avec cette multiplication de ses usages potentiels, de nombreuses questions sont soulevées quant à la capacité de cette technologie à monter en puissance (changement d'échelle dans les temps de latence pour incrémenter des blocs dans la chaîne) : un des enjeux sera donc de disposer de méthodes pour évaluer la qualité et la fiabilité du service.

À cela s'ajoutent des questions environnementales. En effet, le consensus basé sur des arguments cryptographiques et sur des règles protocolaires, qui est le fondement de la confiance décentralisée elle-même à la base de cette technologie, s'avère par nature gourmand en calcul, en stockage – et donc en énergie.

Par ailleurs, la *blockchain* ne se limitant pas aux crypto-monnaies, il peut s'agir, suivant le cas d'usage considéré, d'une implémentation publique, privée ou hybride. Les enjeux ne sont dès lors pas nécessairement toujours les mêmes : par exemple, dans le premier cas, l'anonymat des émetteurs de transactions est requis, pour des raisons de sécurité. Dans l'autre, on souhaitera, au contraire, une identification du requérant. De ce fait, les questions de la garantie de confidentialité ne se poseront pas dans les mêmes termes et il en sera de même des sujets de protection des données personnelles, d'évaluation de la chaîne de confiance du nouveau système et de méthode d'enrôlement de ses acteurs.

Enfin, une attaque lancée en juin 2016 contre un contrat intelligent d'Ethereum, par l'exploitation d'une faille dans le code, a permis à un utilisateur indélicat de tenter de subtiliser 3 millions d'« ethers » (la monnaie virtuelle de cette plateforme), soit environ 36 millions de dollars. Cela a changé la perception de facilité que certains acteurs pouvaient avoir eue jusque-là de cette technologie, qui n'est pourtant pas facile à appréhender, même en ayant des connaissances poussées en technologies de l'information.

Cet avertissement sans frais s'avère intéressant, parce qu'il montre que les mécanismes de sécurité doivent être évalués si l'on veut que la technologie puisse répondre à des critères de maturité. Surtout, il marque la fin d'une doctrine dans laquelle la technologie se suffirait à elle-même sans qu'il fût nécessaire d'y associer un dispositif de gouvernance. À ce titre, il y a eu un débat intéressant et intense au sein de la communauté pour comprendre si l'on pouvait ou non scinder de façon délibérée une chaîne pour réparer l'erreur, et éviter ainsi le versement frauduleux de l'argent – et, si oui, qui avait le droit d'agir ? C'est ainsi que la question de la gestion d'éventuels conflits d'intérêt est apparue.

La Commission européenne, consciente de l'intérêt et des enjeux que présentent ces nouvelles techniques, vient de mettre en place un groupe de travail autour des « Fintechs », la *blockchain* et sa normalisation y sont pointées comme un sujet essentiel. La Commission souhaite s'appuyer sur les organismes de normalisation européens pour évaluer les besoins liés aux spécificités de l'Europe et mettre en place, si besoin en est, un programme de travail.

Dans ce contexte, les enjeux pour la normalisation tels qu'ils ressortent des débats tenus à l'Afnor, où l'écosystème français de la *blockchain* (y compris la famille des *start-ups*) est bien représenté, portent en particulier sur :

- le besoin d'harmoniser une terminologie et un vocabulaire communs ;
- le lien avec l'identité numérique pour gérer la confidentialité entre intervenants et contenus, avec un cas d'usage concernant des dispositions techniques de gestion des données répondant aux exigences du nouveau règlement européen RGPD (Règlement général sur la Protection des Données) relatif à la protection des données personnelles [3] ;
- le besoin de gouvernance pour faciliter le déploiement des *blockchains* dans un cadre maîtrisé ;

(2) Voir, par exemple, les travaux du groupe BIPS : https://github.com/bitcoin/bips

(3) L'atelier CEN ISAEN est une initiative de l'association française AETERNAM soutenue dans le cadre de la collaboration franco-allemande sur la normalisation de l'économie numérique.

- la nécessité d'organiser la répartition des travaux entre, d'une part, un référentiel normatif générique applicable à tout secteur et, d'autre part, des déclinaisons par secteur, dont le secteur financier qui a commencé à réfléchir sur la normalisation d'applications « FinTech » ;
- donner un cadre de référence concernant l'interopérabilité, la portabilité et la sécurité d'usage.

Une opportunité : le nouveau comité technique ISO TC 307 « *Blockchain and electronic distributed ledger technologies* »

À la demande de son membre australien, l'organisme de normalisation international ISO a décidé en septembre 2016 de créer un nouveau comité technique, dont la mission sera de développer des normes génériques transversales à tous les secteurs et s'appliquant aux technologies de la notarisation distribuée.

Les réunions tenues à l'Afnor depuis l'été 2016 montrent que les acteurs français, qui comprennent des *start-ups*, voient dans l'initiative de l'ISO une opportunité pour que la normalisation apporte des réponses en termes de confiance afin que la *blockchain* se développe en tant que technologie accompagnant la transformation numérique, même si elle ne saurait répondre à elle seule à tous les enjeux de cette transformation.

Les discussions qui ont eu lieu lors de la première réunion de l'ISO/TC 307 (tenue en Australie début avril 2017) ont démontré que les acteurs internationaux sont sur la même longueur d'onde à ce sujet. Un consensus indéniable s'établit autour du fait que la consolidation de la confiance dans les nouvelles applications *blockchain* requiert que des travaux soient menés sur les thématiques suivantes :

- de terminologie ;
- d'architecture de référence (distinguer le réseau du service) ;
- de classification des cas d'usage ;
- de sécurité et de confidentialité des données personnelles ;
- de gestion des identités ;
- des contrats intelligents.

Au travers de ces travaux, les acteurs économiques cherchent à sécuriser leurs investissements, sans brider pour autant l'innovation apportée par la technologie.

En conclusion, la *blockchain* est née dans un esprit de rupture s'inspirant d'idées libertaires. Pour autant, afin de progresser en maturité et de gagner la confiance de toutes les parties intéressées, la *blockchain* devra s'appuyer sur une normalisation volontaire. Par rapport à l'offre des consortiums qui s'emparent de la *blockchain* pour produire nombre de spécifications souvent foisonnantes, l'ISO, tout comme l'*International Electrotechnical Commission* (IEC), dispose d'atouts décisifs en matière de confiance, car les normes volontaires que ces organisations élaborent sont de portée internationale et s'inscrivent dans la durée. Elles sont extensibles, car elles sont maintenues à long terme par un processus maîtrisé de façon à être suffisamment générique. À condition d'y contribuer activement, l'ISO et/ou l'IEC, en se positionnant de façon complémentaire aux initiatives *d'open source*, sont à même d'apporter à l'ensemble des acteurs, privés comme publics, et ce, internationalement, des réponses aux défis d'organisation, de portabilité, d'interopérabilité et de sécurité que la *blockchain* devra relever.

Sécurité et insécurité de la *blockchain* et des *smart contracts*

Par Jean-Pierre FLORI
Expert en cryptographie à l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

La sécurité des nombreuses applications utilisant les *blockchains* repose non seulement sur la façon dont sont construites les *blockchains* sous-jacentes, mais aussi sur les spécificités de l'application construite à l'aide des données stockées dans ces *blockchains*, ainsi que sur le comportement des entités participant à l'expansion de la *blockchain*. Dans cet article, nous nous intéresserons à ces différents niveaux de sécurité et nous les illustrerons en nous appuyant sur deux applications phares des *blockchains* : la crypto-monnaie bitcoin et l'ordinateur-monde d'Ethereum.

Introduction

Les *blockchains* sont un élément central de la monnaie cryptographique bitcoin, de l'ordinateur-monde Ethereum, ainsi que de nombreux projets récents. La sécurité de telles applications repose non seulement sur la façon dont sont construites les *blockchains* sous-jacentes, mais aussi sur les spécificités des applications construites à l'aide des données stockées dans ces *blockchains*.

La sécurité des *blockchains*

Pour aborder la sécurité apportée par les *blockchains*, il est tentant de réduire la *blockchain* à sa plus simple expression. On obtient alors un concept d'une simplicité, et même d'une pauvreté technique, extrême : c'est une liste chaînée où chaque nouveau bloc pointe vers le précédent bloc. Si une telle construction est constamment utilisée en informatique afin de stocker des données, elle n'apporte aucune garantie de sécurité sur les données stockées dans un environnement malveillant et il est encore plus malaisé de partager et de mettre à jour une telle structure de données de façon distribuée.

La rigidité des *blockchains*

Si aucun mécanisme de sécurité n'est mis en place, comment s'assurer qu'un bloc de la liste n'a pas été remplacé par un autre bloc ? Il est donc tout d'abord nécessaire de « rigidifier » la liste chaînée.

Cette rigidité est généralement obtenue en incluant dans le $n^{ième}$ bloc de données une empreinte numérique du $i\text{-}1^{ième}$ bloc de données de taille fixée (par exemple, 256 bits) calculée en appliquant à ce dernier une fonction H de hachage cryptographique publique et non paramétrée par un secret, telles que SHA-2 ou SHA-3 (les choix possibles sont encore plus nombreux). La propriété attendue de la fonction de hachage cryptographique est la résistance au calcul de seconde préimage : pour remplacer un bloc N au sein de la liste, il faudrait en effet être capable de trouver un autre bloc ayant le même haché que celui stocké dans le bloc N+1. Les fonctions de hachage sont bien heureusement spécialement conçues pour qu'il soit illusoire d'espérer pouvoir réaliser une telle opération.

Une telle structure peut alors être utilisée comme registre. Les blocs ajoutés deviennent immuables : en remontant depuis le dernier bloc ajouté à la chaîne, il est possible de s'assurer qu'aucun des blocs précédents n'a fait l'objet d'une substitution.

La mise à jour des *blockchains*

Le défi technologique majeur des *blockchains* réside dans la distribution d'un tel registre. Il faut s'assurer que l'ensemble des acteurs s'accordent sur une version commune de la *blockchain*, mais aussi empêcher des entités malicieuses de prendre le contrôle de l'ajout de blocs à la *blockchain*. Ce problème, qui a déjà été beaucoup étudié par les informaticiens, dans le cadre des modèles dits « à permission » (c'est-à-dire de modèles où l'ensemble des acteurs sont connus et contrôlés) est connu sous le nom du « problème des généraux byzantins ».

S'il existe de nombreux protocoles permettant de parvenir à un consensus dans un cadre maîtrisé où tous les acteurs sont préalablement connus, ceux-ci ne fonctionnent plus quand des acteurs non authentifiés peuvent prendre part au protocole, ou s'en désister à leur gré. La principale innovation de bitcoin est d'avoir proposé un protocole permettant de parvenir à un consensus dans un tel environnement « sans permission » en utilisant des puzzles cryptographiques appelés « preuves de travail ».

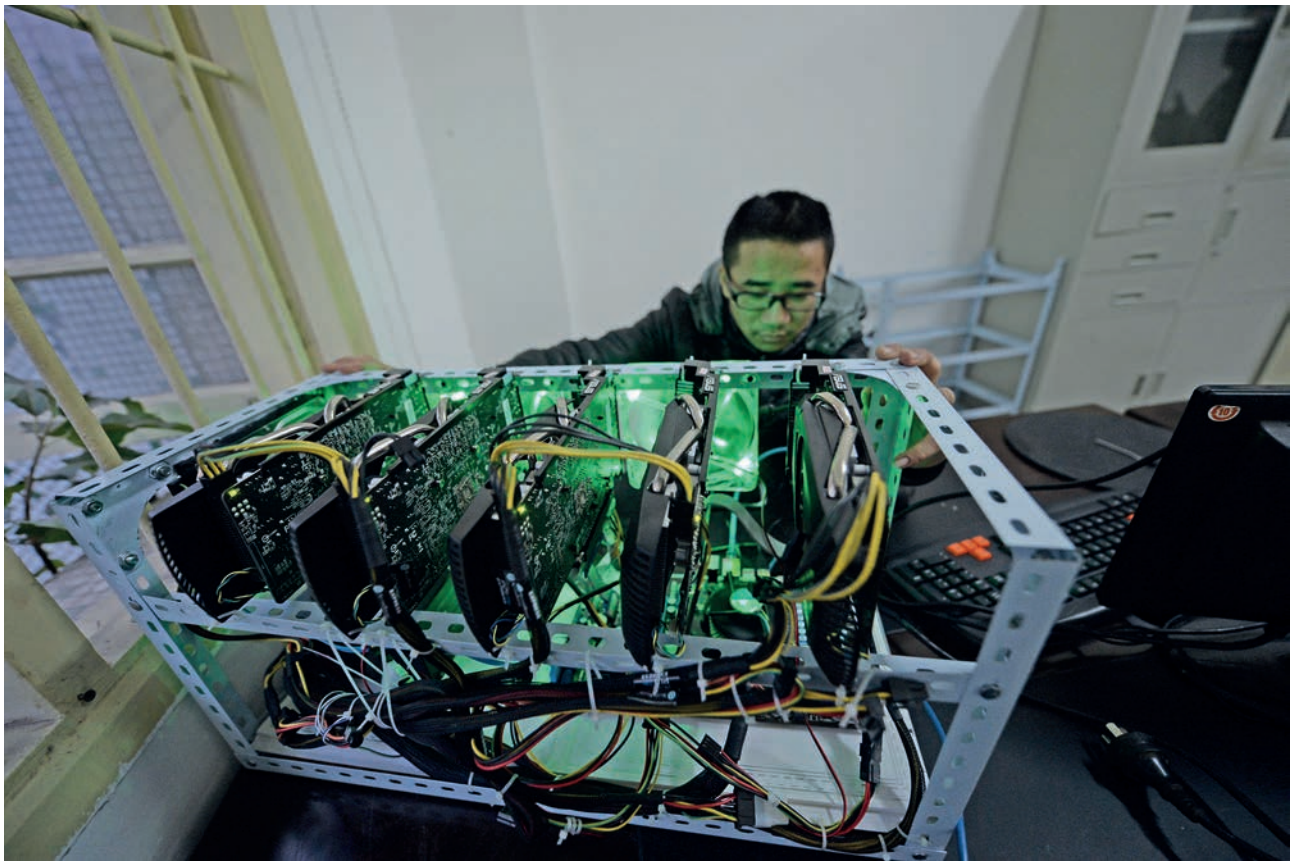


Photo © Ran Wen/Featurechina-ROPI-REA

Un employé de Landminers devant un ordinateur dédié au minage de bitcoins, une activité dans laquelle cette société est spécialisée, Chongqing (Chine), 6 décembre 2013.

« Le fait que la difficulté de la résolution du puzzle cryptographique soit suffisamment grande est un paramètre important de sécurité. »

L'utilisation de « preuves de travail »

Le principe de la « preuve de travail » est le suivant : afin de pouvoir proposer un nouveau bloc valide à ajouter à la *blockchain*, il faut résoudre un problème difficile.

Dans le cas du bitcoin, ces preuves de travail font à nouveau intervenir des fonctions de hachage cryptographiques ! Étant donné le haché H(Bi-1) du bloc précédent de la *blockchain,* ainsi que les données à intégrer au nouveau bloc Bi (une liste Li de transactions à valider dans le cadre de bitcoin), il s'agit essentiellement de trouver un préfixe Ni, tel que le nouveau bloc Bi=(Ni, H(Bi-1), Li) constitué de la concaténation de ces éléments satisfasse la condition que le haché H(Bi) commence par i bits nuls. Ce problème (encore plus difficile à résoudre que le problème évoqué dans le paragraphe précédent) se rapproche du problème de calcul de première préimage d'une fonction de hachage. Pour toutes les fonctions de hachage cryptographiques modernes, il n'existe à ce jour pas de meilleure façon de résoudre ce problème que de tirer des valeurs de Ni au hasard et de calculer le haché correspondant (plus exactement, il est possible d'omettre quelques tours de la fonction de hachage). Il suffit alors de jouer sur la valeur de i pour faire en sorte qu'un nouveau bloc soit généré toutes les dix minutes environ (i vaut aujourd'hui environ 70, dans le cas du bitcoin).

En soi, l'utilisation d'une « preuve de travail » ne permet pas de s'accorder lorsque deux blocs valides sont diffusés à travers le réseau, au même moment. Dans cette éventualité, et pour converger vers un consensus, bitcoin préconise de commencer par « ne rien faire » : chaque nœud choisit aléatoirement un des deux blocs valides pour prolonger sa copie locale de la *blockchain* et travaille dessus (on parle alors de « branche », ou « *fork* »). Avec le temps, il est fortement probable qu'un de ces deux choix conduira à une *blockchain* strictement plus longue que l'autre et le consensus sera alors que tous les nœuds se rabattent sur la *blockchain* la plus longue.

Le fait que la difficulté de la résolution du puzzle cryptographique soit suffisamment grande est un paramètre important de sécurité : tant qu'une entité malicieuse ne contrôle pas plus de la moitié de la puissance de calcul en obtenant ainsi une probabilité strictement supérieure à ½ de générer un bloc avant les autres nœuds, il paraît plausible (mais non prouvé de façon formelle !) que cette stratégie permette de se prémunir d'une entité essayant de réécrire l'histoire en créant sa propre « branche » à partir du nœud de son choix et en y ajoutant de nouveaux blocs jusqu'au moment où ladite branche deviendra plus longue que la « branche » officielle. En particulier, cette stratégie permet de se prémunir des doubles dépenses (un utilisa-

teur transfère une première fois ses fonds, attend que suffisamment de blocs soient ajoutés à la *blockchain* afin que le bénéficiaire considère la transaction comme confirmée, puis réécrit l'histoire pour remplacer le transfert initial par un autre), mais aussi de prévenir la censure (un attaquant pourrait produire une « branche » plus longue dès qu'une transaction qu'il ne voudrait pas voir apparaîtrait).

La sécurité formelle

Un axe de recherche actuel est de formaliser un tel protocole tout en prouvant de façon formelle sa sécurité. Parmi les notions de sécurité formalisées, notons :

- la cohérence spatiale : différents acteurs honnêtes doivent partager la même vision de la *blockchain* officielle (ou au moins un préfixe commun, afin de prendre en compte une légère désynchronisation ou de brefs « *forks* ») ;
- la cohérence temporelle : au cours du temps, la *blockchain* d'un acteur honnête doit conserver un préfixe fixe (c'est-à-dire que sa vision de la *blockchain* ne peut changer que marginalement, à la fin de la chaîne) ;
- la croissance : la longueur de la « chaîne » officielle croît tant qu'un nombre suffisant d'acteurs y contribue ;
- la qualité : une proportion satisfaisante des blocs générés par les acteurs honnêtes finit toujours par être intégrée à la chaîne.

Notons que tous ces travaux posent encore des restrictions plus ou moins fortes sur la modélisation du réseau reliant les acteurs et sur la dynamique de la population des acteurs. Cependant, ils proposent d'autres améliorations par rapport au protocole original du bitcoin afin d'accélérer la vitesse moyenne de validation des blocs en utilisant des chaînes secondaires et en mélangeant protocoles de consensus « à permission » et « sans permission ».

L'attaque des 51 %

Un certain nombre de crypto-monnaies alternatives dont la puissance de minage est moindre que celle du bitcoin ou d'Ethereum ont été attaquées par des groupes qui ont pu réécrire la *blockchain* et dépenser plusieurs fois leurs avoirs en regroupant des puissances de calcul supérieures à 51 % de la puissance de minage. C'est, par exemple, le cas de Krypton et de Shift, qui sont des clones d'Ethereum.

La sécurité du bitcoin

Bitcoin propose de construire une crypto-monnaie au-dessus de la *blockchain* en stockant dans chaque bloc un certain nombre de transactions monétaires. Chaque acteur possède un couple de clés (l'une étant publique et l'autre privée) de signature cryptographique et chaque transaction est représentée en utilisant un langage de script très simple reposant essentiellement sur l'instruction « transférer les bitcoins de la transaction y vers l'adresse z », accompagnée d'une signature « s », où :

- l'adresse z est (le haché d')une clé publique de signature ;
- le numéro de transaction pointe vers une transaction antérieure dans laquelle des bitcoins ont été transférés à la clé publique correspondant à la clé privée ayant produit la signature « s ».

La sécurité des transactions

Afin de dépenser les bitcoins transférés à l'adresse z, il faut être capable de produire une signature cryptographique à l'aide de la clé privée associée, ce que seul le possesseur de ladite clé pourra faire si le mécanisme cryptographique de signature sous-jacent est sûr et, bien évidemment, si cette clé privée n'a pas été divulguée ou dérobée.

Il existe de nombreux schémas de signature cryptographique adéquats. La plupart reposent sur des problèmes mathématiques tels que la factorisation de grands nombres entiers ou la résolution du problème du logarithme discret dans des groupes. C'est sur ce deuxième problème que s'appuie le mécanisme de signature cryptographique utilisé par bitcoin. Plus précisément, bitcoin s'appuie sur la difficulté de la résolution du logarithme discret sur une courbe elliptique à travers le mécanisme de signature ECDSA ***(****Elliptic Curve Digital Signature Algorithm)****.***

Le regroupement des « mineurs »

Un effet pervers de l'utilisation de « preuves de travail » (en dehors du côté hautement énergivore du minage) est que la majeure partie de la puissance de minage se concentre dans des zones proches de celles où sont produits les *Application-specific Integrated Circuits* (ASIC) et où l'électricité est bon marché.

De plus, les acteurs particuliers s'adonnant encore au minage n'ayant pas la puissance de calcul nécessaire pour espérer rentabiliser leur investissement énergétique se regroupent habituellement au sein de « piscines » de minage. Un serveur central centralise les calculs effectués par l'ensemble des mineurs de la piscine et leur redistribue les gains de manière proportionnelle. Le responsable du serveur central a alors un contrôle complet sur la puissance de calcul des mineurs de sa piscine vis-à-vis de l'extérieur.

Il n'est donc pas exclu qu'un acteur unique puisse finir par posséder plus de la moitié de la puissance de minage, remettant en cause le modèle sur lequel repose la non-malléabilité de la *blockchain*.

Des principes différents ont été proposés afin de pallier ces problèmes, tels les preuves d'espace (« *proof of space* ») ou les preuves de possession (« *proof of stake* »).

Les clients « légers »

Une autre dérive des utilisations des bitcoins remet en question le modèle entièrement distribué sur lequel repose la confiance dans cette crypto-monnaie. Afin de s'assurer qu'une transaction est valide, chaque acteur devrait stocker l'intégralité de la *blockchain* afin de s'assurer de la validité des transactions le concernant. Cette chaîne représente aujourd'hui plusieurs gigaoctets de données, et ne serait-ce que le fait de l'obtenir requiert beaucoup de temps. Pour cette raison, des clients dits légers sont apparus qui ne stockent pas la *blockchain* et préfèrent s'adresser au reste du réseau pour s'assurer qu'une transaction a bien été effectuée.

La gestion des portefeuilles

De nombreux utilisateurs préfèrent déléguer la gestion de leur portefeuille, et donc celle de leurs clés privées, à des sites spécialisés. Ces derniers deviennent donc des cibles de choix pour des attaquants cherchant à dérober ou à détruire des crypto-monnaies. De nombreuses attaques de ce type ont été perpétrées contre des sites de stockage et d'échange de bitcoins, tel le site d'échange de crypto-monnaies MtGox. Aucun recours technique n'est possible dès lors que le tiers dit « de confiance » n'est plus capable de restituer les clés secrètes des clients.

La sécurité d'Ethereum

Ethereum utilise la *blockchain* de la même façon que bitcoin : des utilisateurs proposent d'ajouter des transactions et celles-ci sont regroupées en blocs par des mineurs qui vérifient la validité des transactions et cherchent ensuite à résoudre un puzzle cryptographique pour ajouter officiellement le nouveau bloc à la chaîne. Tandis que bitcoin utilisait un langage de script simple de transfert monétaire, Ethereum permet d'utiliser un langage de script Turing-complet, et ainsi de déployer un « ordinateur-monde ». Chaque « transaction » permet de créer ou d'exécuter un programme de façon distribuée entre tous les mineurs. Cette richesse s'accompagne malheureusement de l'introduction de nouveaux problèmes de sécurité, qui ne sont plus d'ordre cryptographique mais d'ordre informatique et qui concernent la sûreté des langages de programmation.

Ethereum Virtual Machine et *Solidity*

Les données stockées sur la *blockchain* permettent de déterminer l'état courant de l'*Ethereum Virtual Machine*, une machine virtuelle complètement distribuée. À chaque utilisateur, mais aussi à chaque programme stocké dans la *blockchain*, est associée une variable « balance » représentant la quantité de crypto-monnaie en sa « possession ».

Afin de faciliter la conception des programmes destinés à être déployés sur l'*Ethereum Virtual Machine* (EVM), un langage de haut niveau nommé Solidity est utilisé, avant d'être compilé. Cependant, la sémantique d'appel de fonctions de Solidity est assez complexe. En particulier, chaque programme peut définir une fonction de « *callback* » qui sera appelée ou non, en fonction de la syntaxe utilisée.

L'attaque contre DAO

Le principe du programme DAO était relativement simple : recevoir de divers utilisateurs des dons destinés à un autre utilisateur, puis transférer à l'utilisateur final ces dons quand celui-ci en fait la demande (c'est une forme de cagnotte virtuelle).

Le code du programme peut être simplifié et ramené à deux fonctions :

- « *donate (address)* », qui enregistre le fait que la quantité de crypto-monnaie renseignée lors de l'appel de fonction est maintenant associée à l'adresse (*address)* dans un tableau interne au programme DAO ;
- « *withdraw (amount)* », qui permet à un utilisateur de demander au programme DAO de lui reverser une [certaine] quantité (*amount)* de crypto-monnaie.

Malheureusement, la syntaxe utilisée par le programme DAO avait la propriété d'appeler la fonction de « *callback* » du programme appelant. Ainsi, un utilisateur malveillant pouvait écrire un programme demandant le retrait d'une somme légitime en appelant « *withdraw* », dont la fonction de « *callback* » émettait un appel similaire permettant de récupérer deux fois la somme due, tirant ainsi profit d'un « *bug* » dans le programme originel.

Conclusion

Les aspects sécuritaires des *blockchains* et de leurs applications sont nombreux et une faille à n'importe quel niveau de la chaîne peut avoir des conséquences catastrophiques. Avant de parvenir à un niveau de maturité et de confiance permettant des applications critiques, de nombreuses innovations sont encore nécessaires.

La (ou les) *blockchain*(s), une réponse technologique à la crise de confiance

Par Arnaud MANAS
Ingénieur, docteur en économie et en histoire, chercheur associé à l'Université de Paris I – Sorbonne (IDHES)
et Yoram BOSC-HADDAD
Spécialiste de la gouvernance des initiatives émergentes et du pilotage économique

Dans sa forme canonique, la *blockchain* est un refus des tiers de confiance. Cette technologie repose sur une posture idéologique qui n'est pas exempte de populisme. Ce refus des institutions établies s'explique en partie par la crise de confiance que traversent les sociétés modernes. Le solutionnisme technologique qui voudrait établir la confiance par algorithmes, sans ancrage social ou juridique, est illusoire. Compte tenu des coûts et des risques, l'usage de la *blockchain* canonique (sans tiers de confiance) présente peu d'intérêt en dehors d'un nombre limité de domaines. En revanche, la mise en œuvre des technologies *blockchain* par des institutions dépositaires de confiance, à l'intérieur d'un cadre juridique et social, paraît promise à un bel avenir. Mais seule une veille active permettra à ses acteurs d'en bénéficier pleinement.

Introduction

Créer un cadastre dans l'ancienne République « très très démocratique » du Gondwana après le départ de son président-fondateur ne serait probablement pas tâche aisée. Dans ce pays (imaginaire) bien connu pour sa corruption, la transposition d'une administration « à l'occidentale » serait probablement vouée à l'échec. En effet, les cadastres classiques sont coûteux, peu efficaces, peu résistants à la corruption et leur fonctionnement est relativement opaque. De plus, ils n'ont pas effectué leur mue technologique post-Internet.

Pour d'aucuns, la « révolution de la *blockchain* » permettrait sans nul doute de résoudre le problème. La solution serait de créer un wiki-cadastre transparent et certifié par la communauté informatique mondiale reposant sur la *blockchain* canonique respectant les cinq critères de Caseau-Soudoplatoff [1]. Ainsi, le Gondwana disposerait d'un cadastre moderne sans infrastructure étatique ni tiers de confiance, et ce, pour un faible coût.

Cependant, un tel projet issu du solutionnisme technologique et sans lien avec la réalité sociale risquerait de finir comme un « éléphant blanc 2.0 ». L'acceptation et la diffusion de la *blockchain* repose sur la confiance. Or, cette dernière ne peut être réduite à un algorithme. Une hybridation est donc nécessaire entre les mécanismes traditionnels et les technologies *blockchain*. Celle-ci permettra de surmonter la crise de confiance que traversent les sociétés modernes et d'offrir de nouvelles opportunités technologiques.

Crise de confiance des sociétés modernes et solutionnisme technologique

La *blockchain*, assemblage habile de protocoles et de primitives cryptographiques adossées à Internet, apparaît comme une solution idéale moderne au problème de la confiance. Les solutions sociales (publicité foncière, dépositaires, banques centrales…) qui ont été élaborées par le passé semblent doublement critiquables au nom de l'efficacité et de la perte de confiance dans les institutions.

Il faut reconnaître que les institutions en place sont souvent conservatrices et lentes à profiter des innovations technologiques. De même, la perte de confiance est un phénomène bien réel. Comme le montrent Yann Algan et Pierre Cahuc [2], une méfiance croissante gagne les pays

(1) CASEAU Y. & SOUDOPLATOFF S., « La Blockchain*, ou la confiance distribuée », Fondapol.org, 2016.*
(2) ALGAN Y. & CAHUC P., La Société de défiance : comment le modèle social français s'autodétruit*, ENS, 2007.*

occidentaux, et plus particulièrement la France. La crise financière de 2008 et l'affaire Snowden de 2013 ont singulièrement accentué ce divorce entre les citoyens-consommateurs et les institutions : « *Trust no one* ».

Après le bitcoin, la *blockchain* est apparue comme un recours face à des institutions discréditées. Son caractère « antisystème » et « anti-*establishment* » répond à la renaissance d'un certain populisme. Cette réponse technologique à la crise de confiance qui mine les sociétés modernes repose sur une logique anarcho-libertaire et sur l'imaginaire historique des mineurs d'or individualistes de la Ruée vers l'Or du XIXe siècle. À la croisée du refus de l'État des libertariens et du communautarisme « technophilique », la *blockchain* est l'incarnation contemporaine d'une vision où la conjonction d'intérêts – voire de vices – privés produirait de la vertu publique. Elle s'oppose non seulement à l'État et à la conception régalienne de l'intérêt public, mais aussi aux mécanismes traditionnels de la confiance et de la régulation par le droit.

Il est intéressant de noter que, de manière analogue, la période des années 1930 avait vu se développer de nombreuses initiatives dans le domaine de la monnaie qui ne sont pas sans présenter certains parallèles avec le bitcoin et avec la *blockchain*. En particulier, la monnaie fondante (WIR [3] et expérience de Wörgl [4]) et la technique de l'estampillage, qui ont vu le jour à cette époque, avaient inspiré une littérature considérable. Ces mécanismes sont largement retombés dans l'oubli avec la guerre.

Paradoxalement, la défiance envers les individus et les institutions va de pair avec une confiance dans les systèmes informatiques et dans la technologie algorithmique de la *blockchain*. Cette confiance s'apparente à une foi quasi religieuse dans la mesure où les protocoles et l'économie du système sont difficiles à appréhender. Dans de nombreux esprits, il existe un parallélisme entre la *blockchain* et Facebook. Les deux sont nés de l'Internet social sur lequel, dans une certaine mesure, les « amis » d'un réseau « likent» une transaction, créant ainsi une « multitude anonyme de confiance ».

Dans sa forme canonique, la *blockchain* propose de remplacer des individus ou des institutions dépositaires de la confiance (droits et devoirs) au nom de l'intérêt général par une communauté immatérielle d'individus mus seulement par leur intérêt individuel. Cette approche anhistorique présente des risques.

Un détour par la monnaie

Parmi les institutions sociales, la monnaie fiduciaire est probablement celle qui repose le plus sur la confiance. La monnaie est une lente construction sociale éprouvée par des crises. Elle repose sur des technologies, mais son fondement essentiel est le droit et la construction juridique. La technologie de la monnaie fiduciaire est faillible : le faux-monnayage est une réalité et aucune technique, qu'elle soit typographique, papetière ou autre, n'éliminera les contrefacteurs. Néanmoins, il reste à un niveau socialement acceptable grâce au Code pénal, qui réprime le faux-monnayage, et grâce aux services de police, qui poursuivent les faussaires. À l'opposé, le bitcoin est construit en dehors de l'État et professe une confiance illimitée dans la technologie. Comme le souligne Hayek [5], la conception *a priori* de constructions sociales est périlleuse. La foi aveugle en la technologie pose un problème de responsabilité : si un *hacker* casse le système, personne n'est véritablement responsable ni en charge de la lutte [6]. La formule « *Code is law* » est trompeuse, à cet égard. L'essor du bitcoin repose en partie sur le « dégagisme » bancaire et institutionnel, sur un refus du « système ».

Ce mouvement de défiance qui semble clair depuis plusieurs dizaines d'années correspond peut-être à la phase descendante d'un cycle d'Hirschman [7], selon lequel les sociétés alternent engagement public et repli vers la sphère privée accompagné de défiance sociale. Dans ce cas, le cycle finira par s'inverser et des institutions réinventées retrouveront des formes de confiance [8].

Enfin, il est primordial d'éviter l'écueil du solutionnisme qui part du constat qu'il est naturel de vouloir utiliser le plus largement possible les nouveaux outils indépendamment de leur utilité marginale : « pour un marteau, tous les objets ressemblent à des clous ». Il se pourrait que l'intérêt suscité par la technologie de la *blockchain* soit une manifestation du solutionnisme qui réduit tout problème à la recherche exclusive d'un algorithme, alors que d'autres mécanismes mixtes alliant des dimensions à la fois sociales, juridiques et technologiques pourraient mieux répondre à la question posée.

Des opportunités technologiques pour répondre à la tension croissante entre monopoles institutionnels et aspirations modernes

Faire confiance au darwinisme

Dans le cadre de notre propos, la crise de confiance dans les institutions se nourrit de trois sources :

- Internet porte en germe une vision libertarienne reflétant son émergence soixante-huitarde et son ancrage californien ;
- les institutions en situation de monopole de droit ou de fait, malgré des améliorations et des modernisations notables (comme les actes authentiques électroniques) sont souvent des tiers de confiance inefficaces au regard des aspirations de la société de l'immédiateté, de la transparence et du *peer-to-peer*.

(3) http://www.alpesolidaires.org/le-cercle-de-cooperation-economique-wir-une-monnaie-suisse-depuis-1934
(4) Voir l'article Wikipedia sur Wörgl et http://www.alterinfo.net/L-experience-de-monnaie-fondante-de-Worgl-a-pris-fin-il-y-a-75-ans-Une-solution-pour-des-temps-de-crise_a29371.html
(5) VON HAYEK F., Scientisme et sciences sociales*, Plon, 1953.*
(6) Ethereum Wikipedia et https://bitcoinmagazine.com/articles/rejecting-today-s-hard-fork-the-ethereum-classic-project-continues-on-the-original-chain-here-s-why-1469038808/
(7) HIRSCHMAN A., Bonheur privé, action publique*, Fayard.*
(8) Il est intéressant de noter qu'Airbnb ou eBay avec leur système de notation n'ont fait que reprendre et moderniser l'ancienne technologie de confiance qu'était la lettre de recommandation. De même, on peut trouver un parallèle entre la blockchain *et la suite d'endos qui crée une chaîne ininterrompue de transferts de propriété et de responsabilité.*

Paradoxalement, la multiplication des transactions désintermédiées, au sens classique, mais passant par des plateformes de « confiance » (dont BlaBlacar et Airbnb sont des archétypes) éduquent le consommateur digital à prendre des risques si la valeur perçue lui semble suffisante et si les commentaires sont globalement favorables.

Cette crise et l'espoir de profits élevés à terme conduisent à un foisonnement d'initiatives et d'investissements pour répondre à travers la *blockchain* à des problématiques de transactions C2C, et, par diffusion, B2B ou pourquoi pas X2Y2Z.

Il y a probablement une bulle comparable à l'explosion de l'Internet dans les années 1990 : au minimum ce sont 80 % des *start-ups* de la *blockchain* qui vont mourir [9]. Mais « l'exaptation » – c'est-à-dire le fait qu'un caractère sélectionné, au sens darwinien, par un bénéfice initial finisse par prospérer sur d'autres bases – nous semble un scénario plus probable que l'extinction dans l'œuf.

Les technologies *blockchain* plutôt que la *blockchain*

Nous considérons que les freins que sont la vulnérabilité, la puissance de calcul, les besoins en énergie, l'absence de gouvernance et les conséquences négatives en termes d'emploi [10] vont limiter les « vraies » *blockchains* à peu de cas se situant souvent en marge de la légalité. Nous pensons, en revanche, que les composantes technologiques de la *blockchain* vont permettre, à terme et à une échelle large, de reconstruire des infrastructures de transaction et de partage à moindre coût, et ce, avec des performances très supérieures, en termes :

- d'automatisation (par exemple, agent de transfert pour l'échange de parts de fonds [11] ou les crédits documentaires) ;
- de temps de latence pour l'enregistrement (de quelques mois aujourd'hui, pour la publicité foncière, à quelques millisecondes, demain, avec un contrat automatique) ;
- et, sans doute encore davantage, d'accès transparent et immédiat à une information authentifiée.

Ignorer le foisonnement créatif (ou, pire, le combattre) serait donc prendre le risque de passer à côté du potentiel élevé d'innovation des briques technologiques de la *blockchain*.

C'est dans ce sens que nous interprétons, par exemple, le projet Hyperledger (Linux Foundation) ou l'approche d'Ethereum.

Les scénarios plausibles

Entre le tiers de confiance « canal historique » lent, opaque et inefficace, et le « machin » distribué anonyme dans le *darkWeb*, il y a de la place pour des tiers de confiance réinventés.

Des consortiums vont probablement émerger pour proposer des solutions hybrides, à l'instar de ce qui s'est fait par le passé pour les systèmes de paiement ou de compensation, mais, cette fois, sans opérateurs centralisés, avec une approche du tiers de confiance très différente et des solutions ouvertes et transparentes (à l'instar de ce qu'est un Blablacar ou un Airbnb par rapport à une chaîne d'hôtels ou à un transporteur public).

En revanche, le rythme d'émergence des modèles économiques viables nous semble encore très incertain.

Des impératifs prospectifs pour les institutionnels, pour les opérateurs installés et pour les *start-ups* qui veulent durer

Dans cet environnement, les stratégies extrêmes sont très risquées, et ce, pour tous les acteurs :

- Attendre, c'est prendre le risque de passer à côté d'une disruption réelle ou de continuer à investir massivement dans une infrastructure dont la valeur peut chuter brutalement ;
- Tout miser sur la *blockchain*, c'est combiner risque technologique et risque financier, sauf, bien sûr, pour les *start-ups* et leurs investisseurs, qui viseraient de « pivoter [12] » en se revendant rapidement à un consortium institutionnel.

Il est préférable, dans une logique prospective, de se donner les moyens, d'une part, d'une veille active pour comprendre en profondeur le sujet et, d'autre part, de l'apprentissage par l'expérimentation focalisée et répétée pour se confronter à un monde réel, lui-même en mouvement.

En particulier :

- pour les institutions, il s'agira d'embrasser les besoins de transparence et de vitesse en ayant des stratégies de couverture permettant de contrôler (si possible) les émergences sur les points de faiblesse ;
- pour les *start-ups* qui veulent durer, il nous semble important de cristalliser leur essence comme fournisseurs de briques de savoir-faire technologique ou comme créateurs/développeurs de nouveaux usages ;
- pour tous, il nous semble essentiel de favoriser la création de consortiums d'expérimentation confrontant ces logiques, et d'incubateurs verticaux qui soient des creusets d'émulation et de raffinement des savoirs sur les usages des technologies *blockchain*.

Conclusion

Au vœux de Jean-Paul Delahaye : « Imaginez […] un très grand cahier que librement et gratuitement tout le monde puisse lire, sur lequel chacun puisse écrire, mais qui soit impossible à modifier et indestructible [13] ! », on peut ajouter : « Imaginez des gardiens du registre dépositaires d'une mission d'intérêt général, responsables devant la Loi et la société [14], chargés de l'interprétation des

(9) MOUGAYAR W. : http://www.ibtimes.co.uk/ethereums-william-mougayar-successful-ico-not-indicative-success-ico-1607859
(10) TAPSCOTT in *McKINSEY, May 2016,* How blockchains could change the world.
(11) Les Échos*, « Gestion d'Actif », 4 avril 2017, SCHAFROTH E., « La* Blockchain *s'invite dans la gestion d'actif ».*
(12) Au sens lean start-up.
(13) DELAHAYE Jean-Paul, « Les Blockchains*, clé d'un nouveau monde »,* in Mathématiques et mystères*, Belin, 2016, p. 40*
(14) Le faux en écritures publiques ou authentiques est puni de 10 ans de prison, contre 3 ans pour un faux « ordinaire ».

règles ! ». Croire que les algorithmes règleront tout est illusoire, car l'expertise juridique et la responsabilité sociétale sont nécessaires chez des dépositaires de confiance.

Est-il vraiment nécessaire de choisir entre le dépositaire de confiance « à l'ancienne » et la *blockchain* moderne informatisée reposant sur une communauté immatérielle anonyme ?

En alliant la technologie du registre signé, transparent et accessible sans coût à la confiance envers des individus ou des institutions insérés dans la société, le meilleur des deux mondes est possible.

Laissons donc manches de lustrine, registres jalousement conservés et refus idéologique des tiers de confiance. Préparons-nous à créer un ensemble de technologies et de concepts alliant confiance sociale et algorithmique pour réaliser, avec une signature digitale, des partages horizontaux et transparents, en toute responsabilité et à la vitesse d'Internet.

Un nouvel outil numérique pour la fiabilisation des *supply chains* : *la blockchain*

Par Matthieu HUG
Serial entrepreneur, cofondateur et CEO de Tilkal

Les registres numériques distribués *(blockchains*) promettent de réinventer la confiance en rendant possibles des systèmes de notariat désintermédiés et décentralisés. Leur application à l'industrie financière, largement étudiée et commentée, pourrait modifier nos systèmes d'échanges basés sur des tiers de confiance.
D'autres applications de ces technologies visent, quant à elles, non pas simplement à se substituer aux mécanismes de confiance existants, mais bien à établir de la confiance là où celle-ci fait défaut. Une application ayant un intérêt sanitaire majeur est l'assurance de la traçabilité des produits de bout en bout, depuis le fabricant jusqu'au consommateur : d'abord pour fournir au consommateur la transparence qu'il réclame sur ce qu'il consomme, et la conformité, dont il veut pouvoir juger, par rapport à ses critères de santé ou d'éthique. Ensuite pour lutter contre l'incroyable croissance de toutes les formes de contrefaçon, qui touchent toutes les industries, du médicament aux aliments pour nourrissons, en passant par les pièces automobiles.

Depuis quelques années, les différentes formes de commerce illicite (contrefaçon et « marchés gris ») sont devenues la première manifestation de criminalité mondiale, avec un « chiffre d'affaires » de l'ordre de 1 000 milliards de dollars (qui les place bien avant le trafic de drogue). Ce que l'on croit cantonné au luxe dans l'imaginaire collectif européen concerne en réalité toutes les industries : du médicament aux pièces détachées automobiles, du lait pour enfants aux sachets de parmesan, des téléphones portables aux batteries, des jouets au vin et aux huîtres. Concrètement, à eux seuls, les médicaments contrefaits tuent 700 000 personnes dans le monde chaque année (par comparaison, le SIDA a fait 1,1 million de victimes en 2015). Ainsi, la traçabilité des produits et des biens est devenue un enjeu global de santé et de sécurité publique.

Si le risque reste pour l'instant relativement maîtrisé en Europe occidentale, ce fléau est devenu dramatique ailleurs dans le monde : l'organisme algérien de protection des marques déposées (Inapi) estime que 80 % des produits en vente dans ce pays sont des faux. Selon le laboratoire pharmaceutique Lilly, ce sont plus de 90 % des médicaments vendus en ligne qui relèveraient du commerce illicite. Et cette situation s'aggrave rapidement : globalement, les contrefaçons et les marchés illicites ont connu une croissance d'un facteur 10 au cours des 10 dernières années. Plusieurs éléments expliquent cette situation :

- l'essor du e-commerce (en particulier, des places de marché) a facilité l'écoulement des produits détournés ou falsifiés, générant une forte demande d'approvisionnement en amont ;
- cet appel d'air sur la distribution en ligne a favorisé la structuration d'une véritable chaîne d'approvisionnement illicite à l'échelle globale, couvrant les matières premières, la fabrication, la vente en gros, les transports ou la logistique ;
- ces *supply chains* illicites sont massivement interconnectées aux *supply chains* légitimes, échangeant, mélangeant, substituant des produits à tous les niveaux et à toutes les étapes ;
- l'ampleur du trafic illicite : avec 1 000 milliards d'euros en jeu, ceux qui s'y livrent ont globalement plus de moyens financiers pour l'organiser qu'aucun industriel seul n'en a pour les contrer. Ainsi, lorsqu'en 2013, 28 laboratoires pharmaceutiques mondiaux lancent le financement sur 3 ans d'un programme de lutte avec Interpol, il s'agit de 5,9 millions de dollars, résultant de la saisie de faux médicaments pour 81 millions de dollars en 2015 (à comparer à un marché global du faux médicament de probablement 150 à 200 milliards de dollars…).

En bout de chaîne, l'exigence grandissante de transparence de la part des consommateurs est donc largement justifiée.

Établir la continuité de l'information

Face à l'utilisation du numérique pour globaliser la distribution de produits issus des chaînes illicites, les approches de fiabilisation des chaînes industrielles légitimes ont, à l'évidence, été déficientes. Certes, les dispositifs de marquage physique des produits et des biens se sont développés et même multipliés. Mais alors que les *supply chains* se sont globalisées, les informations issues de ces dispositifs de marquage restent confinées à chaque intervenant : en clair, il n'existe dans pratiquement aucune industrie de connaissance consolidée et fiable du cycle de vie réel d'un produit, qu'il s'agisse de sa localisation à un instant T, de ses conditions de transport, de son lieu de vente ou de son éventuel reconditionnement (*repackaging*).

Cette rupture de la chaîne des informations nous rend aveugles : elle permet les trafics illicites. En la palliant, on peut espérer réaliser deux avancées importantes :

- la création d'une identité numérique du produit constituée de son cycle de vie consolidé. Étant indépendante et de nature différente du marquage physique, cette identité numérique crée les conditions d'une véritable authentification forte des produits ;
- une analyse statistique, grâce à des algorithmes spécialisés, de l'ensemble des cycles de vie permettant de détecter les anomalies, que ce soient des indicateurs de trafics illicites ou des sources d'amélioration du fonctionnement de la chaîne d'approvisionnement.

À partir d'une identification unique opposée sur le produit, les actions effectuées sur celui-ci sont déclarées à chaque étape de sa *supply chain*, depuis sa production jusqu'à son utilisation finale (par exemple, sa provenance, son origine, ses conditions de fabrication ou de stockage, sa mise sur palette, son transport en conteneur, etc.). En bout de chaîne, l'identité numérique ainsi constituée peut être lue par un consommateur (avec un *smartphone*) en s'appuyant sur le marquage unique du produit (par exemple, un QR code). Cette lecture en bout de chaîne est en soi un événement de la *supply chain* qui est lui aussi constitutif de l'identité numérique du produit : on voit que l'on a là, d'ores et déjà, un mécanisme simple et unitaire qui permet de détecter en temps réel des produits inconnus, des reconditionnements anormaux, voire des ventes dans des zones géographiques non autorisées.

La mise en œuvre d'une telle plateforme pose des questions techniques évidentes, mais pas insolubles, de volumétrie d'information et de performance d'accès. Au-delà, elle pose surtout des questions complexes de confiance, au sens large du terme. Tout d'abord, chaque intervenant doit partager des informations relatives à son activité : cela pose une question évidente non seulement de confidentialité, mais aussi de transparence. Ensuite, il y a un risque grave d'effet « pot de miel » : une information centralisée serait inévitablement la cible de cyberattaques et de piratages, compte tenu des enjeux. Il faut donc consolider sans centraliser, et partager tout en garantissant la confidentialité. Enfin, il y a la question de la fiabilité des données.

Pourquoi la *blockchain* ?

Les questions de confidentialité et de consolidation décentralisée amènent naturellement à l'idée d'un registre numérique décentralisé (*blockchain*). Mais cette technologie peut-elle être utilisée à bon escient dans le cadre des *supply chains* et, si oui, comment ?

D'un point de vue fonctionnel, la technologie *blockchain* peut être vue comme une base de données distribuée qui enregistre des transactions séquentiellement dans le temps et interdit leur modification ultérieure : régulièrement, un groupe de transactions est créé, ce bloc référence explicitement le précédent, puis il est soumis à validation, par consensus de tout ou partie des participants au registre. Une fois validé, un bloc devient vite très difficile à modifier, et il en va de même pour toutes les transactions qu'il contient : il faudrait pour cela modifier en même temps tous les blocs ultérieurs et tromper le mécanisme de consensus appliqué par tous les autres participants. D'un point de vue technique, on peut aussi voir la technologie *blockchain* comme un protocole de synchronisation de données opérant directement sur la couche logicielle de plus bas niveau dans un réseau, offrant ainsi une surface d'attaque plus faible que des protocoles de plus haut niveau.

À partir de ces deux points de vue, de nombreuses variations (parfois interdépendantes) sont possibles : mécanismes de consensus, participation ouverte au consensus ou limitée à des membres pré-identifiés, accès public ou privé aux données échangées, celles-ci étant chiffrées ou non, etc. Les configurations choisies varient naturellement en fonction du problème que l'on cherche à résoudre. Dans tous les cas, on voit que la *blockchain* est un composant technologique qui rend un service précis, à savoir l'établissement d'une confiance consensuelle. Celle-ci repose sur deux piliers : sa non-répudiabilité (la donnée peut servir de « preuve ») et son inaltérabilité en tous cas à un coût « raisonnable ». La question cruciale est alors de savoir autour de quelle information, précisément, l'on veut (et l'on peut) établir ce consensus de confiance.

La mise en œuvre

Dans le cas des *supply chains*, on va utiliser un registre numérique distribué et privé à deux fins : organiser un réseau de collecte d'informations et prouver ultérieurement, grâce à celles-ci, l'origine et le contenu de chaque élément constituant l'identité numérique du produit. Ce registre est partagé entre des nœuds qui sont tous connus et identifiés individuellement : ce sont les intervenants de la *supply chain* concernée, typiquement les fournisseurs, les industriels, les transporteurs, les distributeurs, voire les institutionnels. Il va donc s'agir d'une *blockchain* dite « à permission » pour laquelle on peut appliquer un algorithme de consensus plus simple que dans le cas des *blockchains* publiques (et donc bénéficier de performances bien meilleures qu'avec ces dernières).

La collecte des informations auprès de chaque intervenant de la *supply chain* se fait localement, au sein de son

système d'information, *via* un nœud packagé avec une couche d'API (interface de programmation applicative) : l'information est ensuite recopiée par le protocole sur chaque nœud du réseau. Les nœuds du réseau appartenant *a priori* à différents acteurs industriels, chaque information est chiffrée avec une clé propre à chaque nœud afin d'assurer la confidentialité.

On utilise ainsi la *blockchain* pour créer la confiance sur deux dimensions : l'origine de l'information et son inaltérabilité (son intégrité dans le temps). La confidentialité de l'information est gérée par des mécanismes de chiffrement avancés en amont de la *blockchain*. La scalabilité de l'accès aux données ainsi que leur consolidation et leur agrégation statistique sont, quant à elles, gérées en aval sur des données extraites de la *blockchain*, mais qui référencent celle-ci. À aucun moment ne se pose la question de la véracité des informations entrées dans le registre par les intervenants : une information fausse reste une information qu'il est fondamental de capturer. C'est l'analyse de la *supply chain* à partir des informations fournies par les intervenants, que celles-ci soient vraies ou fausses, qui permettra de détecter les « faux » et de les corriger. De fait, l'objectif n'est pas de constituer un registre d'informations « vraies » : cela n'aurait aucun sens, car cela présupposerait que toutes les malveillances et toutes les erreurs auraient été résolues, et donc que le problème initial des *supply chains* décrit plus haut l'aurait été également. L'objectif est de constituer un registre d'informations qui ne soient pas modifiables afin d'être en mesure, en les analysant, de détecter des problèmes et d'établir une boucle de rétroaction transparente, laquelle, progressivement, fiabilisera l'ensemble de la *supply chain* en responsabilisant chacun des intervenants.

Ce mécanisme est notablement évolutif : il n'est pas nécessaire que tous les intervenants de la *supply chain* fournissent de l'information, puisque même une vue partielle permettra d'amorcer la boucle de rétroaction. En outre, un nouvel intervenant qui se connecte au système n'a qu'à déployer son nœud : une fois celui-ci autorisé dans le réseau, le protocole *blockchain* assurera sa synchronisation avec le reste du réseau. Chaque nouvel intervenant connecté au réseau augmente à la fois la sécurité du réseau, la transparence globale et la pertinence de la rétroaction. La *blockchain* est donc un mécanisme propre à unir progressivement des acteurs industriels ayant à la fois des intérêts et des valeurs en commun.

D'autres points sont à traiter pour un déploiement industriel de la *blockchain*, notamment l'archivage des données ou encore le cadre juridique (en particulier en ce qui concerne les données personnelles). Des réponses existent, mais dépassent le cadre de cet article. Au-delà des tests initiaux, la question désormais posée est celle de l'utilisation de cette brique technologique, en conjonction avec d'autres, pour résoudre des problèmes se posant à une échelle industrielle.

Conclusion

Les technologies de registre numérique distribué, ou *blockchain*, apportent une brique de confiance. L'approche envisagée ici n'est pas de chercher à utiliser une technologie pour forcer la confiance entre les participants à la *blockchain*, ni même pour avoir confiance dans les données qu'ils déclarent dans la *blockchain* : cela reviendrait à résoudre à l'avance le problème posé. Dans ce contexte, on crée les conditions pour que les informations ne soient pas altérées : l'intégrité des données, leur quasi immutabilité, est au cœur de la confiance garantie par le registre numérique distribué. Grâce à cette immutabilité, on peut utiliser des algorithmes d'analyse des cycles de vie des produits tels que déclarés par les intervenants d'une *supply chain* et y détecter des signaux faibles caractéristiques d'anomalies, quelle qu'en soit la nature (dysfonctionnement, malveillance, irrégularité, non-qualité, etc.). On génère ainsi une boucle de rétroaction permettant de responsabiliser chaque intervenant et, *in fine,* de fiabiliser le fonctionnement des *supply chains*. C'est une logique d'amélioration continue similaire à une approche de type *lean manufacturing* qui est ainsi mise en place, mais à l'échelle d'une filière industrielle. Cette amélioration continue établit les conditions de la transparence, base d'un nouveau contrat de confiance avec le consommateur.

Références bibliographiques (en ligne)

Eli Lilly & Co, *Integrated Report 2015*, Part Operating Responsibly.

http://fightthefakes.org

International Chamber of Commerce.

OCDE, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*, 2016.

Europe & UN-OHIM, *2015 Situation Report on Counterfeiting in the European Union*, April 2015.

2016, KPMG and AGMA, *Gray Markets Report.*

ONUDC, *Le Trafic illicite de biens contrefaits et la criminalité transnationale organisée*, 2014 : http://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_FR_HIRES.pdf

Smart business networks: the evolution

By Louis-François PAU
Rotterdam School of Management and Copenhagen Business School

The intelligence of an information network is augmented by its functionality (its ability to distribute, store, assemble, or modify information). Transmission networks are technically complex, but business-wise they are "dumb" pipes that transport information without enhancing it. An information network augmented by formalized business relationships can be "smart"; it can improve the utility of information in multiple ways (that is synonymous with creating economic value).
Conversely, a lone transaction between two business partners rarely stands isolated, especially in an electronic commerce context, but the economic value accrues already then for both partners. New transactions can be created with the same or other partners, by cascading whole or parts of the same initial transaction, thus building a network of business relations which develops over time.
To address the two above paradigms, has been defined the concept of "Smart Business Network" (SBN).

A Smart Business Network is a developing web of people and organizations, bound together in a dynamic and unpredictable way, creating economic outcomes from quickly (re-)configuring links between these actors using shared communication and logistic networks [1,2]. Ultimately, smart business networks reshuffle the very notion of linear paths (or graphs) in business processes, to replace it with asynchronous interaction protocols and transactions between parties to the development, and embedding these inside the underlying communication network [3].

Business networks that are "smart", display quick connect and quick disconnect capabilities; they can pick the best capabilities from many business network actors, plug these capabilities together, and make these play in unison; they also control, or own, the business logic for multi-actor execution of business processes.

All three words in the title "smart business networks" are necessary. In management, the adjective "smart" is attributed to an action that is novel and different, hence thought of as innovative. Smart actions create remarkable, "better than usual" business results. "Smart" has a connotation with fashionable and distinguished, but also of being short-lived. The word "smart" in "smart business networks" is therefore not an absolute but a relative term. Smartness is a property whereby the network can create "better" results than other, less smart business networks or other forms of business arrangements. Smart Business Networks develop not only because technology permits them to develop, but more significantly because markets and modern business competitiveness require such networks in order to survive and thrive [1]. Management attention then focuses on managing the network, on the processes for joining or leaving a network, and on processes by which to select suppliers from the network. We can now go one stage further and say that a fundamental competitive capability is to construct and manage a smart business network.

A "smart business network" (SBN) as defined above, has more operationally the following characteristics [3]:

- A group of participating businesses - "partners" or "actors" - that form the nodes, and this group is not necessarily visible to the outside;
- Actors are linked together via one or more communication networks forming the links, or lines, between the nodes;
- Actors are linked together as well by a shared ontology of bilateral attributed agreements or service level agreements (SLA's) of a temporary nature;
- The partners interact in novel ways they could not implement on their own, or possibly with other parties; this is the SBN network benefit, often linked to the mutual partner discovery and by smart network dynamics [4];
- The SBN is perceived by each participant as increasing his own value, even if individual overall goals/utility functions may be different; a simple illustrative case metric

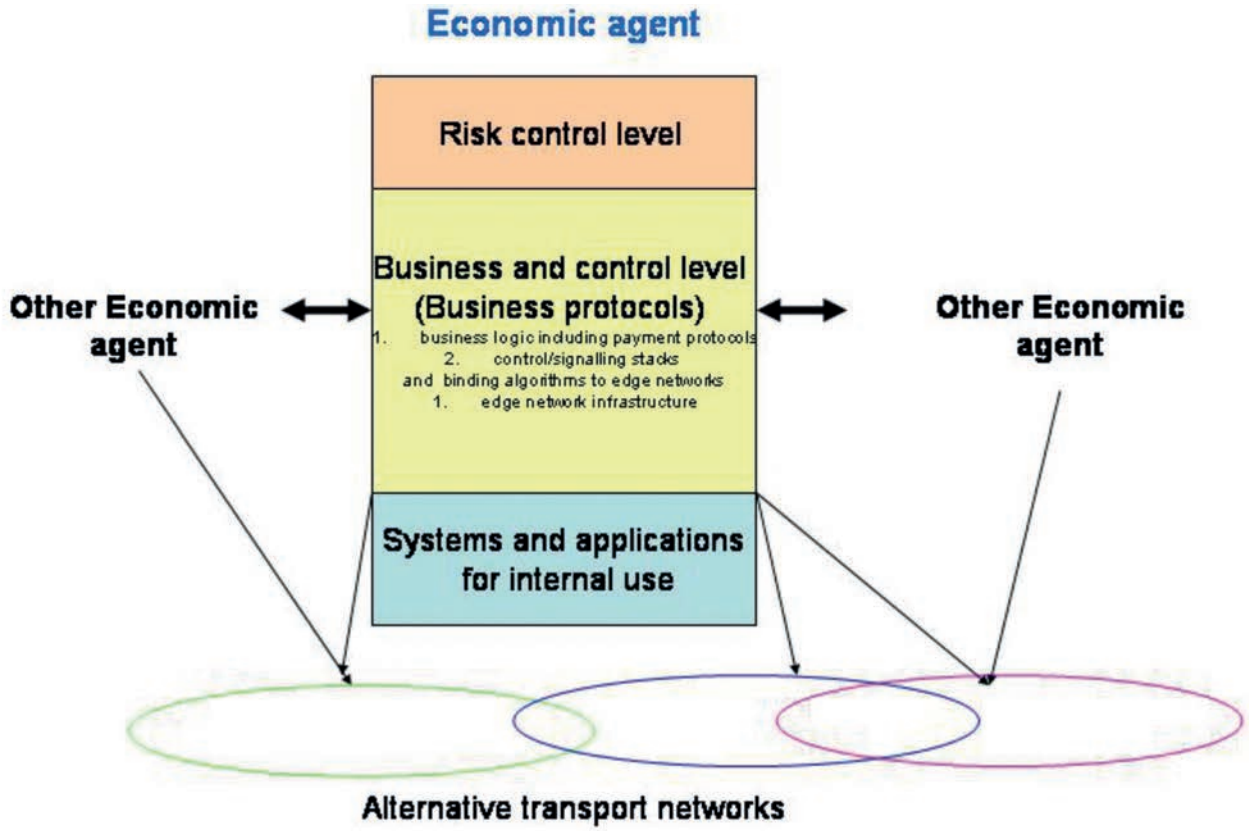


Figure 1: Smart business network at node level, showing the interaction architecture with other partners/nodes, using the interaction networks.

for the utility is the incremental turnover, profit and capacity utilization for each partner when he joins the SBN; the basic equilibrium concept providing governance inside the SBN is one of a non-cooperative Nash game, and not of a collaborative Pareto game. The forces of attraction and repulsion, which generalize the utility, must be measurable between any two partners of the SBN sharing the same ontology; for lack of further data, these forces are set equal to the business outcomes determined by a simple joint bidding auction;

- The SBN is sustainable over some time as a network, subject to agreed-upon termination rules;
- The SBN must normally be resilient if one or more businesses nodes in the network drop out, disappears, or malfunctions.

Figure 1 further specifies at the level of a given SBN partner, the 3-tiered node architecture, where the second level is the one linked to other SBN nodes, sharing as well communications and logistic networks.

Deployments

Whereas some physical supply networks exhibit the attributes of smart business networks, already today most of their attributes can be found for example in [5]:

- mobile content delivery networks, where quick-connect must be done in quasi real-time with content/DRM owners at end user request [3];
- electronic CAD networks, where building blocks get assembled with custom blocks, simulated, tested and prototyped;
- health management insurance networks where specific expertise in a localized way has to be assembled together with service delivery facilities such as clinics;
- mass customization services, such as video-on-demand subscription services, where the customer requests and their time profile shape the sequence of SLA's between content owners, re-purposing services, transport networks, and CRM systems [6];
- support services for software development [7];
- book routing services for bookshops [8]; Upload once for multiple indexing sites; Change inventory pricing for different services; Create subsets of books for various sites; Add information or web site links to each record; Check your data for completeness; Save hours per week/month;
- translation and internationalization services in the UK business [9].

A case from outsourcing in the high-tech sector

The case is a snapshot of the direct implementation of the above approach by one of the world's top management consultancies, to cater to a strategic goal, i.e. turn the company "A", a global high tech systems supplier to the communications & media operator sector, into a systems and service integrator benefiting from the outsourcing

trend amongst its customers. This goal had to be shared across the other parties in the smart business network, before they could possibly join it.

Case specification

More precisely, the case is about designing a smart business network around the field support, installation and consulting Division of the company "A", to allow "A" to achieve a significant worldwide market share in communications and media distribution network operations amongst its worldwide public operator customers, at a time where these customers change their core business; they shift from running networking services to the new core business of interconnecting networks they do not want to operate themselves any more. This can only succeed if, on a global scale, "A" can identify, select, use and sever links to a wide diversity of smaller technology or skills suppliers, many of them only operating in localized markets, or having de facto only one key customer. Vice-versa, these smaller suppliers find a resilient business in supplying "A" on a repetitive basis. As the outsourcing opportunities are time-critical, and as "A" wants to leverage its systems know-how (about its own products and those of selected other ones), financial terms are in effect of secondary importance compared to the ability to bid fast and comprehensively. Very often the track record of the smaller high tech companies may have been with competitors to "A" or with "A"'s own customers without any direct connection to "A". The potential number of partners in the total smart business network is about 500, with, on a country or regional basis, a minimum of three and maximum of about 15. The capabilities mapped out to model the business logic fell into the broad ontological categories of: skills sets, available staff on short or medium term notice, prior systems/product/tools experience, incentives and penalty conditions, geographical distance of pockets of skills sets to the operators' sites, etc.

Case discussion

The smart business network approach of Section 1 was found to be extremely powerful and relevant, first because of the shear automated exhaustive handling of all possible partner configurations, with their evolutions over time (from known track records into fulfilment horizons on the outsourcing contracts) [4]. Next, the possibility for "A", with help of the consulting company, to tailor the forces of attraction and repulsion between partners (usually via simple look-up tables expressing real capabilities) allowed to select efficiently the partners in different bidding situations.

One drawback was the learning time it took for traditional management consultants to adapt to this novel way of thinking; but actually this time was far less than the time "A"'s sourcing division would have taken to tackle the same volume of analysis. The other drawback was the reluctance by some of the 500 possible parties to disclose some capabilities and track record characteristics; but actually this was never a show-stopper, as information was readily available by indirect channels such as the business references these same companies were citing.

The outcome parameters were (cost, delay, quality) KPI's in supplying outsourcing contracts to operators as single but ever changing smart business networks. So far, over 10 joint bids to operators have not lead to questions on the methodology, but rather on the goals and organizations of the operators.

Implementation frameworks

To realize the three following properties of smart business networks:

- quick connect and disconnect between actors;
- pick, plug and play;
- business network specific business logic.

Fortunately some open standards developed over the last 10 years offer the required tools. They include BPM process specifications, OMG Model driven architecture (with its evolution), open mediating ontologies (such as SymOntoX), XML specifications, and Web Services [10]. A number of commercial tools also exist, such as e.g. Microsoft BizTalk, IBM WebSphere, BEA WebLogic or Tibco ActiveEnterprise. At the network level, and this was one of the key contributions to smart business networks, the idea is to use extensions to the IP signaling protocols (such as DIAMETER), by the IEEE P1520 network interface standard, to carry out the asynchronous partner search and matching. BPM protocols between partners have to be tailored to a domain, and [3] provides a simple example in the form of SNMP Simple Network management protocol, with a payment function and due authorization when the required resources are made available.

The next frontier: managing intellectual property rights as smart business networks

Today, more and more joint ventures or co-developments extend the notion of individual supply transactions to reach the development of the intellectual property rights (IPR) supporting a joint product or service development; sometimes even, the above discussed business logic (Figure 1) becomes an element of the intellectual property of the smart business network. One of the difficulties is that a lot of legal and technical expertise must go into the crafting of the intellectual property right claims and their ownership. At the same time, co-development should not be at the expense of development times and of blocking the licensing to third parties. This is especially true in the case of SME's who want to offer their IPR to some parties, while needing some from yet other parties.

The Swedish company Upgötva AB [11] has embarked into a setting up an IPR brokering platform using basic IPR attributes filled out by the IPR owners, and managing ontologies and matching tools to create smart business networks. In this way, third parties can discover not just what IPR is available, but also the complementary needs inside a product or service business network.

Conclusion: risks involved in smart business networks and some research challenges

As process events can be linked very quickly, and economic agents may recompose themselves and/or their capabilities, the dynamic resource optimization across many economic agents can become overly complicated. We suggest that some genetic and bio-informatics algorithms may be useful to realize the corresponding attraction-repulsion selection, and to execute in a distributed way the recalculations of the business benefits inside the shared SBN network.

Smartness may emerge spontaneously and not be intentionally designed; and conversely, if designed smartness may not deliver its promises, it may enhance some business risks. While much theoretical and experimental research is still needed to identify the causal relations leading to smart business network risk formation, some of the underlying forces are the following [12]:

- Bounded group rationality that limits the actors' group mind sharing in a same way as for individuals;
- Dynamic emergence and decay of key information brokers, information creators, and information users. Measurement on SBN networks shows that most nodes can be categorized as one of these three types;
- Sometimes lack of agreed upon and transparent confidence, governance, and trust maintenance procedures inside a SBN;
- Changing behaviors due to the SBN networking itself; cases have already shown that when a company organized itself as a smart business network across business units, it ultimately disappeared as the entities felt their accountability, initiatives, discipline, focus and expertise did not require the same attention as this was "taken care of by others in the network";
- What should be the granularity of the operations at each smart business network partner when networked? Too high granularity leads to overlaps, inefficiencies and conflicts, while too low granularity reduces innovation and flexibility; the notion discussed here is not the one of modularity in a linearized supply chain, but instead about the range of the specialized activities at each business partner in a smart business network, which can be formalized by task graph decomposition within a network.

References

[1] VERVEST P. H. M., HECK E., PREISS K. & PAU L.-F., "Emergence of smart business networks", *Journal of information technology* (JIT), vol. 19, 2004, pp. 228-233.

[2] VERVEST P. H. M., HECK E., PREISS K. & PAU L.-F., "Introduction to smart business networks", *Journal of information technology* (JIT), vol. 19, 2004, pp. 225-227.

[3] PAU L.-F. & VERVEST P. H. M., "Embedding business logic inside communications networks: a network based business process management", in VERVEST P. H. M., HECK E., PRICE K. & PAU L.-F. (Eds.), "Smart business networks", *Springer Lecture series in Computer Science*, September 2004, 15 p., www.springer.de/comp/lcs

[4] PAU L.-F., "Discovering the dynamics of smart business networks", *Computational Management Science*, vol. 11, Issue 4, 2014, pp. 445-458, http://dx.doi.org/10.1007/s10287-013-0162-x

[5] VERVEST P. H. M., HECK E., PREISS K. & PAU L.-F., *Smart business networks* (Eds.), Springer, Berlin, ISBN: 3-540-22840-3, 2005, 442 p.

[6] CHEN H. & PAU L.-F., "Mass Customization in Wireless Communication Services: Individual Services and Tariffs", in PILLER F. T. & TSENG M. M. (Eds.), *Handbook of research in mass customization and personalization* (in 2 Volumes: vol. 1: *Strategies and Concepts*, vol. 2: *Applications and Cases*), World Scientific, Singapore, 2010, http://www.worldscibooks.com/business/7378.

[7] HEIKKILÄ J., HEIKKILÄ M., LEHMONEN J. & PEKKOLA S., "Smart ICT support for business networks", in (5).

[8] http://www.bookrouter.com

[9] http://www.thebigword.com

[10] WERTHNER H., FODOR O. & HERZOG M., "Web information extraction and mediation as a basis for smart business networking", in (5).

[11] Upgötva AB, Stockholm, Suede.

[12] PAU L.-F., "Smart business networks: interaction-coordination aspects and risks", *Business Process Management Journal*, vol. 18, n°5, pp. 829-843, http://dx.doi.org/10.1108/14637151211270180

Blockchains and smart contracts: The technology of trust?

Introduction

Jean-Pierre Dardayrol

1 – Blockchains

The blockchain: The concept, techniques, interested parties and uses

Côme Berbain, assistant manager in Expertise, Agence nationale de la sécurité des systèmes d'information (ANSSI)

Blockchains are a fad. This hard-to-ignore word is frequently used with varying acceptations! To grasp this new phenomenon, the effort must be made to define it, identify its structural components and check on the relevance of its properties and promises. Given the multitude of experiments in several branches of the economy, we wonder whether the term "blockchain" relevantly applies to certain uses. We also wonder about the motivation that leads various parties to take interest in this phenomenon. Far from being merely technical, the fundamental issues of blockchain technology have to do with organization and governance, with the finding of solutions for trustworthy transactions among human beings. In this sense, this new technology has a part in the digital transition in several areas, especially the legal professions.

The economic stakes of blockchains

Patrick Waelbroeck, professor, Télécom ParisTech – Institut Mines-Télécom

Blockchain technology extends far beyond time stamps, bitcoins and the security of financial transactions. An ecosystem involving smart, connected objects (the Internet of things) probably cannot develop without some form of this technology, which opens the way toward a "liquefaction" of the physical world, an economics of real-time microtransactions and the smart sharing of data bases. However it is important to distinguish between types of blockchains, in particular private and public ones, since they have quite different economic properties. The problems related to the governance of public blockchains suggest that this technology cannot, by itself, create trust.

Blockchains? The challenges of implementation

Ilarion Pavel, engineer from the corps des Mines (Conseil général de l'économie, de l'industrie, de l'énergie et des technologies) and Laboratoire de physique théorique (École Normale Supérieure)

Blockchains encounter several technical, legal, societal and regulatory difficulties during implementation. These problems are reviewed; and a few solutions, suggested.

2 – Uses and the transformation of business and industry

2.1 Le financial sector

Distributed register technology: What impact on the financial infrastructure?

Alexis Collomb, chair of Finance (Conservatoire national des Arts et Métiers, CNAM), **Klara Sok**, researcher and doctoral student (CNAM), and **Lucas Léger**, researcher and doctoral student (CNAM)

There has been much talk about how distributed register technology, in particular blockchains, will transform the financial infrastructure. By focusing on payment systems and the infrastructure, this article seeks to discover the reasons why parties in the financial sector have been prudently enthusiastic about this technology. The problems of adopting it and hesitation about doing so are discussed, in particular the presupposition of a new paradigm, "coopetition". A concise inventory of recent initiatives by payment institutions, banks (in particular central banks) and international institutions explores this technology's possibilities, in particular that of putting it into production. The prospects…

Blockchains, the Bank of France and the ACPR

Nathalie Beaudemoulin, coordinator of Pôle FinTech Innovation (Autorité de Contrôle prudentiel et de Résolution), **Didier Warzée**, engineer from the corps des Mines, expert at Pôle FinTech Innovation (Autorité de Contrôle prudentiel et de Résolution), and **Thierry Bedoin**, chief digital officer (Banque de France)

The ACPR (Autorité de Contrôle prudentiel et de Résolution), which oversees banks and the insurance industry in France, and the Bank of France (the central bank) are coming to grips with the technological revolution under way in financial services. Blockchains figure among the techniques that call for optimizing, or even modifying, the processing and delivery of financial services. However this technology is not very mature. It must cope with four major dilemmas before it can be used for financial operations.

Blockchains, a lever of digitization for investment banks

Éric **Rossignol**, in charge of quantitative analysis and of Innovation Laboratory (Department Securization at Crédit Agricole CIB), and **Xavier Laurent**, member of the team Innovation and of the department Strategy & Business Transformation, and leader of the Blockchain Community (Crédit Agricole CIB)

The reason investment banks are designing so many prototypes using blockchain technology is that their business heavily depends on the trust they bring to customer relations. Trust is the driving force in blockchain technology. Till now, investment banks have seen this technology as an opportunity for curbing costs and delivering a better service to customers rather than as a threat. After all, firms still need a supplier of liquidity at the best price…

How is the French Post Office, a long trusted institution, tackling blockchain technology with the help of IRT SystemX?

Alain Roset, La Poste; and **François Stephan**, assistant general manager in charge of development et international affairs at the Institut de Recherche Technologique (IRT) SystemX

Some pundits are predicting that blockchains will deeply change the nature of trusted third party relationships. The digital revolution and the "power of the multitude" have made this possible. According to some experts, this new breakthrough technology has the power to radically alter business models, not only those that have prevailed for decades or centuries but also more recent ones. A historically trusted party for centuries now, the French Post Office (La Poste) has been staking out an ever stronger position on the Internet and in the field of digital trust services, thus warranting its role as a trusted third party in both the real and virtual worlds. Since 2014, it has invested in blockchain technology. In 2016, it formed a partnership with IRT SystemX, a research institute with industrial and academic credentials, the goal being to accelerate its cycle of innovation thanks to this new technology.

The operation of a blockchain

Gautier Marin-Dagannaud, engineering student at Télécom ParisTech-Institut-Mines Télécom and Master's student at École polytechnique, currently at Ledgys

Blockchains are a disruptive technology. To gauge its potential, we must understand how it operates by examining its original use for bitcoins. A blockchain is a distributed register, i.e., a ledger divided among actors on a network. Like any register, transactions will modify entries in the ledger; and users must be identified. Unlike nearly all current registers however, a blockchain works without a central controlling authority… whence several issues and technical problems.

2.2 The culture and entertainment industries

Blockchains and smart contracts: A first round of feedback from the music industry

Christophe Waignier, director of resources and strategy, Société des auteurs, compositeurs et éditeurs de musique (SACEM)

For fifteen years now, the music industry has been at the center of the digital revolution. Blockchain technology has stirred up debate among recording artists and other players in this industry, in both the United States and Europe. Start-ups and, too, traditional actors, such as the SACEM in France, are conducting experiments. The first results have attracted interest and opened new perspectives for collaboration among parties in the culture and entertainment industries. In the short run however, this emerging technology is still too frail to be used as a lever for accelerating the music industry's digital transformation.

Art objects and blockchains

Jurgen Dsainbayonne, founder of Seezart

The art market is undergoing digitization. Several factors are at work: the impact of the new technology, the changing profile of art collectors (turnover of generations) and the 2008 financial meltdown, which, by upending the bond market, reinforced the view of art as a financial asset. Digitization has also exposed the flaws of a system that is, rightly or wrongly, deemed to be opaque and cliquish. Several scandals have broken out about intellectual property rights, authenticity and the origins as well as value of artworks. This is the context where blockchain technology, owing to its inherent properties, can boost confidence, make digital transactions secure and respond to the issues that have cropped up on this changing market.

Chains of books and blocks

Arnaud Robert, director of legal affairs, groupe Hachette Livre

Apart from a few experts and experiments, blockchain technology is still "promising". Among these promises are the new uses owing to its purported characteristics: the qualities of being open but unforgeable and of being reliable even in the absence of a trusted third party to a transaction. The book market could make its digital activities much more efficient if this technology were to keep its promise of being an inviolable register, a secure means for transferring files, or even an automatic machine for authorizing, controlling and collecting royalties. For it to be the revolutionary tool announced, it must keep its most far-reaching promise, namely: being a peer-to-peer tool at everyone's service instead of a toy in the hand of new monopolistic middlemen.

2.3 Other uses

Blockchains at the service of public actions

Malo Carton, engineer from the corps des Mines, Agence des participations de l'État (APE); and **Pierre Jérémie**, engineer from the corps des Mines, head of the risk-prevention service (direction régionale et interdépartementale de l'environnement et de l'énergie, DRIEE) in Île-de-France

Thanks to blockchains, decentralized registers can be designed; and trust in the validity of these registers, shared among concerned parties. Inherent in this technology is a decentralization of the data bases underlying blockchains. For public authorities, this decentralization marks a shift of paradigm away from the usual organization whereby public data are stored by public operators subject to close oversight. This article presents two fields where the application of blockchain technology is under study: a new chain of more fluid financial securities that are easier to control; and the possibility of keeping the records of easements so as to better inform buyers on the real estate market.

The Internet's infrastructure and services

Stéphane Bortzmeyer, engineer in the Department of Information Systems, Association Française pour le Nommage Internet en Coopération (AFNIC)

Several applications have been proposed for blockchains. In many cases however, the description of the actual use of blockchains is so vague that we are unable to assess whether or not it is reasonable to have recourse to this new technology. Blockchains are not useful for any- and every application. Herein, two widely discussed applications related to the Internet's infrastructure come under discussion: computer logs and the registry of filenames. How to make a registry using blockchains? What are the advantages, problems and obstacles?

MakerNet: Distributed manufacturing

Pierre-Alexis Ciavaldini, student-entrepreneur, École 42, and cofounder of BlockFest

"Release early, release often!" This well-known saying in the computer world comes from The Cathedral and the Bazaar (1997). This basic book on the open source movement has shed light on the competitive advantages gained from this new vision of digitization. This philosophy, when applied to material objects, leads to designing a new model – distributed manufacturing – that will be made secure thanks to blockchain technology. France has offshored its cutting edge industries and lost much of its know-how in microelectronics. Meanwhile, electronics has become a form of craftwork in Shenzhen. As a result, dozens of new smartphones, called shanzai, are created day after day: a sort of open standardized hardware, which exists only in China. MakerNet proposes generalizing this model to other cultures through an ecosystem of distributed manufacturing, a possibility offered by blockchains.

Blockchains and smart contracts: Prospects for the Internet of things and e-health

Philippe Genestier, PhD in Microelectronics, Orange Labs; **Loïc Letondeur**, engineer in R&D, Orange Labs; **Sajida Zouarhi**, engineer and doctoral student in information sciences and networks at Orange Labs and Laboratoire d'informatique de Grenoble, LIG, INP); **Alain Prola**, inventor/developer of applications for Androïd; and **Jean-Marc Temerson**, research engineer, head of projects at Orange Labs, now retired

Given the growing use of objects connected through the Internet of things (IoT) and the increasing interconnection of heterogeneous systems producing myriads of personal data, our digital society faces new questions about: the decentralized and "mixed" administration of these things, resilience, confidentiality of the access to data, traceability of uses, etc. Blockchain technology replies by proposing: a decentralized organization, procedures for reaching a consensus that satisfies diverging interests, and a sharing of trust – since the trusted third party is no longer a single person. New opportunities will arise in a sharing economy based on social networks 2.0, where connected human beings and things will interact without any difference being made between the two. Blockchains can drop "anchors" between the physical and virtual worlds: an operation or transaction in the real world will thus have a counterpart in the digital realm. Though not answering all questions, blockchain technology is appropriate whenever trust, transparency and traceability are indispensable. Let us not fail to mention, however, what blockchains cannot do, namely: verify the authenticity of registered data or the legitimacy of "nonelectronic" operations.

3 - Smart contracts and oracles

Regulating smart contracts and the regulator's smart contracts

Catherine Barreau, professor at the Faculty of Law and Political Science: Université de Rennes 1, IODE UMR CNRS 6262, Université Bretagne-Loire

Sooner or later, a technological innovation becomes a matter of law. Users of the innovation –those who benefit from it but also those who fall victim to it –demand regulations. Blockchains are quietly entering the legal world in the field of corporate financing. Smart contracts, though still of limited use, should soon join them. Since they are so complex that their development depends on a secure legal framework, the nature of this new sort of contract must be defined; and its uses, determined. Although most uses are private, we can imagine a public use by regulatory authorities…

Smart contracts… legal aspects

Éric **Barbry**, attorney, director of the Digital Law Pole, Cabinet Alain Bensoussan Avocats Lexing

Smart contracts are not a new, nor the opposite of idiotic contracts. To tell the truth, they are not even contracts. They are a way of encoding a contract and making its application automatic, therefore, easier, faster and surer. Smart contracts rely on blockchain technology, which interests several branches of the economy: finance, music, and services involving middlemen, depositories or trusted third parties. Like any technique, smart contracts have advantages, but they also raise questions. What about security? And, too, programming errors?

Blockchains and smart contracts in the culture and entertainment business

Jérôme Pons, consultant on digital technology and strategies in the culture and entertainment business and delegate on blockchain standardization at Music won't stop

Contracts are omnipresent in the culture and entertainment business, in particular in the film, video and music industries. Nonetheless, whether passed with authors, producers, publishers or distributers, they are not always applicable or executed. The minimum sums guaranteed under a contract might transfer an "excessive" share of the value toward producers and editors; and the absence of legal metadata might reduce the amount paid to the rightful owners (e.g., performing artists). Is it utopian to imagine a contract that is programmed and executed automatically so as distribute a "fair" share of the value to the creators, producers, editors, distributors and consumers of digital contents and to provide a remuneration to the rightful owners that reflects consumption (via down-

loading or audience ratings)? Blockchain technology is part of the answer…

Oracle hardware, the layer of trust between blockchains and the physical world

Vanessa Rabesandratana, customer success manager, Ledger; and **Nicolas Bacca**, chief technical officer, Ledger

Blockchain applications are evolving in a totally virtual environment that has been designed to be fully separate from the real world. Smart contracts, decentralized applications and cryptocurrencies have a limited hold on the physical world around us. We can even describe these two universes as existing on planes that are never superimposed. Each use of this technology thus raises the following questions: How can blockchain applications interact efficiently and in security with the real world? How can smart contracts tap external data with efficiency and in security? This sort of question cropped up quite naturally from the very first days of this new technology. Tools and interfaces thus had to be adapted. The trusted platform for relating the real world to blockchains has a name: Oracle.

4 - Opportunities and stakes

Why standardize blockchains?

Olivier Peyrat, managing director of Association française de normalisation (AFNOR); and **Jean-François Legendre**, in charge of development at AFNOR

Blockchain technology has a considerable growth potential, since so many uses have been imagined, some of them now being deployed. It will be potentially disruptive, and probably become a strategic issue in several industries. However blockchain technology must first attain a certain level of maturity, whence the need to adopt standards for offering the necessary reassurance about certain aspects of the processes used.

The security and insecurity of blockchains and smart contracts

Jean-Pierre Flori, expert in cryptography, Agence nationale de la sécurité des systèmes d'information (ANSSI)

The security of many blockchain applications depends not just on the construction of a chain of blocks. It also depends on the specific characteristics of the application as it uses the data stocked in such a chain. In addition, it depends on the conduct of the entities involved in the expansion of a blockchain. Two flagships of blockchain technology are used to examine these various levels of security: the crytocurrency bitcoin and the virtual machine Ethereum.

Blockchains, a technological response to the crisis of confidence

Arnaud Manas, engineer, PhD in Economics and History, associate researcher at Université de Paris I - Sorbonne (IDHES); and **Yoram Bosc-Haddad**, specialist on the governance of emerging initiatives and steerage of the economy

In its canonical form, a blockchain eliminates trusted third parties from transactions, thus reflecting an ideological stance tainted with populism. This refusal of established institutions can partly be set down to the crisis of confidence in modern societies. Technological "solutionism" tries to establish trust through algorithms, without any legal or social grounds; but it is an illusion. Taking account of costs and risks, the use of blockchains without trusted third parties has little interest outside a few fields. In contrast, the use of blockchain technology by the institutions that serve as trusted third parties, within an established legal and social framework, is promising since active monitoring and oversight are an indispensable condition for benefitting fully from blockchains.

A new digital tool for making supply chains reliable, blockchains

Matthieu Hug, serial entrepreneur, cofounder and CEO of Tilkal

Distributed digital registers – blockchains – hold the promise of reinventing the conditions for trust through decentralized notary systems without go-betweens. Applying them to the financial industry has been the subject of much study and many comments; such applications could modify systems of transactions based on trusted third parties. Other applications of this technology do not simply replace the existing arrangements but even try to establish trust there where it is in shortage. An application of much interest in the field of health is the tracing and tracking of drugs from manufacturer to consumer. For one thing, consumers will thus obtain the accountability they demand about the products they consume and will be able to judge the product's compliance with health or ethical criteria. For another, such an application will hamper the unbelievable growth of all kinds of counterfeit products in all industries: drugs, automobile parts, baby food…

Smart business networks: The evolution

Louis-François Pau, Rotterdam School of Management and Copenhagen Business School

The intelligence of an information network is augmented by its functionality (its ability to distribute, store, assemble, or modify information). Transmission networks are technically complex, but business-wise they are "dumb" pipes that transport information without enhancing it. An information network augmented by formalized business relationships can be "smart"; it can improve the utility of information in multiple ways (that is synonymous with creating economic value).

Conversely, a lone transaction between two business partners rarely stands isolated, especially in an electronic commerce context, but the economic value accrues already then for both partners. New transactions can be created with the same or other partners, by cascading whole or parts of the same initial transaction, thus building a network of business relations which develops over time.

To address the two above paradigms, has been defined the concept of "Smart Business Network" (SBN).

Issue editor: ***Jean-Pierre Dardayrol***

Blockchains y smart contracts, ¿tecnologías de confianza?

Introducción
Jean-Pierre Dardayrol

1 - Las *blockchains*

La *blockchain*, concepto, tecnología, actores y usos
Côme Berbain, Subdirector adjunto de experiencia de la Agencia francesa de Seguridad de Sistemas de Información (ANSSI)

La *blockchain* está de moda. De hecho, es difícil ignorar este término que se usa en abundancia, con acepciones diversas. Con el fin de abordar este nuevo fenómeno, es necesario tratar de definirlo, identificar sus elementos estructuradores e interrogarse sobre la pertinencia de sus propiedades y promesas.

La multitud de experimentos en un gran número de sectores económicos nos invita a reflexionar sobre la pertinencia de la utilización de la *blockchain* dependiendo de sus casos de uso y de los motivos reales de los diferentes actores.

Los retos fundamentales de la *blockchain*, lejos de ser únicamente técnicos, tienen que ver con la organización, la gobernabilidad y la definición misma de soluciones que permitan responder al problema de la confianza en las interacciones humanas. En este sentido, la *blockchain* es un nuevo instrumento técnico que induce y participa en la transformación digital de muchos sectores, en particular en los oficios relacionados con el derecho.

Los retos económicos de la *blockchain*
Patrick Waelbroeck, Profesor de Telecom ParisTech – Institut Mines-Télécom

La *blockchain* es una tecnología que va mucho más allá del registro de fecha y hora, del bitcoin y de la seguridad de las transacciones financieras. El desarrollo de un ecosistema en torno a los objetos inteligentes conectados no podrá realizarse sin la *blockchain* (bajo una forma u otra). La *blockchain* abre las puertas de la fusión del mundo físico, la economía de las micro-transacciones en tiempo real y la distribución inteligente de bases de datos. No obstante, es importante distinguir los diferentes tipos de *blockchain*, especialmente las *blockchains* públicas de las privadas, ya que sus propiedades económicas son muy diferentes. Por otra parte, los problemas de gobernabilidad de las *blockchains* públicas dejan entrever que la tecnología *blockchain* no puede garantizar la confianza por sí sola.

La *blockchain,* algunos retos de implementación
Ilarion Pavel, Ingeniero jefe de Minas, Consejo General de la Economía, Industria, Energía y Tecnología y Laboratorio de Física Teórica de la Escuela Normal Superior

En este artículo se analizan las dificultades técnicas y otros problemas jurídicos, sociales o reglamentarios que se deben enfrentar durante la implementación de la *blockchain*, y se sugieren algunas soluciones potenciales.

2 - Casos de uso, transformaciones de las empresas y sectores económicos

2.1 El sector financiero

Tecnología de los registros distribuidos, ¿qué impacto tiene sobre la infraestructura financiera?
Alexis Collomb, Catedrático de finanzas del Conservatoire national des Arts et Métiers (CNAM), **Klara Sok**, Investigadora y estudiante de doctorado del CNAM, y **Lucas Léger**, Investigador y estudiante de doctorado del CNAM

Se ha hablado mucho de la tecnología de los registros distribuidos, y en particular de las *blockchains*, que pueden modificar profundamente las infraestructuras financieras. Este artículo, el cual se focaliza en los sistemas de pago y las infraestructuras de mercado, trata de explicar en primer lugar las razones del entusiasmo, aún prudente, de los agentes financieros por esta tecnología. Se analizan también los problemas y la desconfianza que genera su adopción, incluyendo el nuevo paradigma de coopetición que presupone. Posteriormente, se establece un pequeño balance de las últimas iniciativas de las instituciones de pago, bancos (en particular, los bancos centrales) e instituciones internacionales para entender mejor las posibilidades de la tecnología o incluso, en algunos casos, ponerla en marcha. Por último, se presentan sus perspectivas futuras.

Los retos de la *Blockchain* para el Banco de Francia y la Autoridad de Supervisión Prudencial y de Resolución (ACPR)
Nathalie Beaudemoulin, Coordinadora del Centro FinTech Innovation de la Autoridad de Supervisión prudencial y de resolución, **Didier Warzée**, Ingeniero de Minas, especialista del Centro FinTech Innovation de la Autoridad de Supervisión prudencial y de resolución, y **Thierry Bedoin**, Chief Digital Officer del Banco de Francia

La Autoridad de Supervisión prudencial y de resolución (que controla los bancos y las aseguradoras), al igual que

el Banco de Francia han sabido transformarse para poder enfrentar los desafíos de la revolución tecnológica que viven los servicios financieros. La *blockchain* forma parte de los temas tecnológicos que pueden optimizar, e incluso modificar, la materia que alimenta las actividades financieras. Sin embargo, esta tecnología carece de madurez y deberá superar cuatro grandes dilemas antes de poder ser utilizada para realizar operaciones financieras.

La *blockchain*, una palanca de digitalización para los bancos de financiación e inversión (BFI)

Eric Rossignol, Encargado del análisis cuantitativo y del laboratorio de innovación del Departamento de titularización del Crédit Agricole CIB, y **Xavier Laurent**, Miembro del equipo de innovación y del Departamento Strategy & Business Transformation y líder de la Comunidad Blockchain del Crédit Agricole CIB

Los bancos de financiación e inversión (BFI) (o bancos al por mayor) realizan muchos prototipos basados en la *blockchain* ya que sus actividades se basan ampliamente en la confianza que proporcionan a sus clientes. La confianza es también el motor de la *blockchain*. Hasta la fecha, los BFI piensan que la *blockchain* es más una oportunidad para limitar los costes y proporcionar un mejor servicio a sus clientes que una amenaza. En efecto, las empresas todavía necesitan un proveedor de liquidez al mejor precio.

Cómo aborda *La Poste*, un actor de confianza secular, la *blockchain*, con el apoyo de IRT SystemX

Alain Roset, La Poste, y **François Stephan**, Director General Adjunto encargado del desarrollo y de asuntos internacionales del Instituto de Investigación Tecnológica (IRT) SystemX

Algunos dicen que la *blockchain*, nueva tecnología revolucionaria, permitirá un cambio profundo de los terceros de confianza gracias a la tecnología digital y a la potencia de la multitud. Para otros, la *blockchain* parece tener el poder no sólo de modificar radicalmente los modelos económicos históricos, establecidos desde hace décadas o siglos, sino también apoyar modelos económicos muy recientes (igualmente revolucionarios). La Poste, operador histórico de confianza en Francia, afianza desde hace varios años su presencia en Internet y ha puesto en marcha servicios digitales de confianza, confirmando así su papel de tercero de confianza tanto en el universo físico como en el universo digital. Desde 2014, el grupo postal francés invierte en la *blockchain* y en 2016 ha decidido trabajar con IRT SystemX, un instituto de investigación que cuenta con conocimientos laborales y académicos, con el fin de acelerar su ciclo de innovación basado en esta tecnología.

El funcionamiento de la *blockchain*

Gautier Marin-Dagannaud, Estudiante-ingeniero de Telecom ParisTech - Institut-Mines Telecom y estudiante de master de la École Polytechnique, actualmente en Ledgys

La *blockchain* es una tecnología profundamente revolucionaria. Para entender su potencial es indispensable comprender las bases de su funcionamiento a través de su caso de uso original, el Bitcoin. Una *blockchain* es un registro distribuido; es decir, compartido entre los diferentes actores de una red. Como en cualquier registro, hay usuarios, que es necesario poder identificar, y transacciones que modifican el estado del registro. Sin embargo, a diferencia de la inmensa mayoría de los registros actuales, la *blockchain* funciona sin autoridad central de control. Esto implica muchos desafíos y problemas técnicos.

2.2 Las industrias culturales

Blockchains y *smart contracts*, primeros retornos de experiencia de la industria musical

Christophe Waignier, Director de recursos y de estrategia, Sociedad de Autores, Compositores y Editores de Música de Francia (SACEM)

Desde hace más de quince años, la industria musical está en el punto central de la transformación digital. En este contexto, las *blockchains* suscitan naturalmente muchos debates en la comunidad artística y entre los actores de la industria musical, tanto en los Estados Unidos como en Europa. Actualmente, varias experiencias concretas, desarrolladas por *start-ups*, pero también por agentes más tradicionales como la SACEM, comienzan a emerger. Los primeros resultados obtenidos suscitan interés, ya que abren nuevas perspectivas de colaboración entre los diferentes actores de la industria. No obstante, estas tecnologías emergentes siguen siendo demasiado frágiles para poder representar, a corto plazo, una verdadera palanca de aceleración de la transformación digital del sector.

Objetos de arte, los desafíos de la *blockchain*

Jurgen Dsainbayonne, Fundador de Seezart

El mercado del arte ha emprendido en los últimos años una transformación digital. Esta transformación ha sido impulsada por varios elementos: el impacto de las nuevas tecnologías, una renovación generacional del perfil de los coleccionistas, y finalmente la crisis de 2008 que, al afectar el mercado de los bonos y obligaciones, tuvo como efecto un fortalecimiento de la visión del arte como un activo financiero.

Esta digitalización también subraya los fallos de un sistema que se considera, con o sin razón, como opaco y propio a una élite. Ha habido muchos escándalos que implican los derechos de autor, la legalidad, autenticidad, procedencia y hasta el valor mismo de las obras de arte.

Es este contexto, la tecnología *blockchain*, por sus propiedades intrínsecas, puede reforzar y garantizar una confianza digital y responder a los desafíos de un mercado cambiante.

La cadena del libro y las *blockchain*

Arnaud Robert, Director jurídico del Grupo Hachette Livre

Salvo el caso de algunos expertos y algunos experimentos, la *blockchain* aún se encuentra en la fase de promesas. Promesas de nuevos usos posibles gracias a las cualidades principales que se le presta: la de ser abierta y al mismo tiempo a prueba de falsificaciones, ser fiable incluso en ausencia de terceros de confianza.

El mundo del libro podría ganar en eficiencia en sus actividades digitales si la *blockchain* cumple con sus promesas

de registro inviolable, medio seguro de transferencia de archivos, e incluso de máquina automática para autorizar, controlar y cobrar tasas.

Sin embargo, para que constituya la herramienta revolucionaria que pretende ser, será necesario que cumpla con su mayor promesa, la de ser un instrumento de relación entre usuarios, de igual a igual, al servicio de todos, y no el juguete de nuevos intermediarios monopolistas.

2.3 Otros casos de uso

La *blockchain* al servicio de la acción pública

Malo Carton, Ingeniero de Minas, Agencia de participaciones del Estado (APE), y **Pierre Jérémie**, Ingeniero de Minas, Jefe del Servicio de Prevención de riesgos y molestias, Dirección regional e interdepartamental del medio ambiente y energía (DRIEE) de la región Île-de-France

La tecnología *blockchain* ofrece la posibilidad de construir registros descentralizados y compartir la confianza entre los operadores sobre la validez de estos registros. La descentralización de las bases de datos subyacentes a una *blockchain* es inherente a esta tecnología. En el caso de la acción pública, esta descentralización constituye un cambio de paradigma de la organización habitual de datos públicos hasta ahora almacenados por uno o varios operadores públicos vigilados de cerca. En el artículo se presentan dos campos de acción pública, estudiados actualmente, que incluyen la aplicación de soluciones que utilizan esta tecnología: la creación de una nueva cadena de títulos que garantice una circulación de títulos financieros, más fluida pero también más fácilmente controlable, y las posibilidades ofrecidas por la *blockchain* para el registro de derechos y servidumbres sobre los suelos con el fin de información mejor a los compradores.

Las infraestructuras y los servicios de Internet

Stéphane Bortzmeyer, Ingeniero de la dirección de sistemas de información y operaciones de la Asociación francesa para el sistema de nombres de Internet y la cooperación (AFNIC)

Muchas aplicaciones se han propuesto para la cadena de bloques (*blockchain*). Pero cabe anotar que, en muchos casos, la descripción de «cómo» se puede utilizar la cadena de bloques para esta aplicación es tan aproximada que es imposible saber si su uso es, en dicho caso, razonable o no. Sin embargo, esta cadena no es útil para todas las aplicaciones.

El texto presenta dos aplicaciones relacionadas con la infraestructura de Internet: los diarios (en el sentido de diario de a bordo) y, sobre todo, los registros de nombres, cuyo funcionamiento ya ha sido objeto de numerosas discusiones.

¿Cómo puede realizarse un registro de nombres en una cadena de bloques? ¿Cuáles son sus ventajas? ¿Cuáles son los problemas y obstáculos?

MakerNet o la fabricación distribuida

Pierre-Alexis Ciavaldini, Estudiante-emprendedor de la escuela 42 y cofundador del BlockFest

«*Release early, release often!*" Este proverbio conocido del mundo informático proviene de *The Cathedral and the Bazaar* (1997), una de las obras fundamentales del movimiento *open-source* que revela la ventaja competitiva que ofrece esta nueva visión de la informática. Esta filosofía, aplicable al hardware, permite la elaboración de un nuevo modelo de producción distribuida cuya seguridad se puede garantizar gracias a la *blockchain*.

Francia ha deslocalizado su industria de punta y ha perdido gran parte de su *know-how* en microelectrónica. *Por el contrario*, en Shenzhen, China, la electrónica se ha convertido en una forma de artesanía. Gracias a ella China puede crear cada día decenas de nuevos teléfonos inteligentes que se denominan «*Shanzai*», una forma de *open-hardware* estandarizado (que sólo existe allí). MakerNet propone la generalización de este modelo y su apertura a otras culturas a través de un ecosistema de fabricación distribuida posible gracias a la *blockchain*.

Blockchains y *Smart Contracts*, perspectivas para el Internet de las cosas y para la e-salud

Philippe Genestier, Doctor en microelectrónica de Orange Labs, **Loïc Letondeur**, Ingeniero de Investigación y Desarrollo, de Orange Labs, **Sajida Zouarhi**, Ingeniero y estudiante de doctorado en informática y redes de Orange Labs y del LIG (Laboratorio de informática de Grenoble INP), **Alain Prola**, diseñador/desarrollador de aplicaciones Android, y **Jean-Marc Temerson**, Ingeniero de Investigación, responsable de equipo y de proyectos de Orange Labs, jubilado

Debido a la creciente utilización de objetos conectados y la interconexión de sistemas heterogéneos que generan innumerables datos personales, nuestra sociedad digital enfrenta nuevos retos: la administración descentralizada y heterogénea de estos objetos, su resistencia, el respeto de la vida privada en el acceso a los datos, la trazabilidad de los usos, etc.

La *blockchain* propone soluciones a estos desafíos.
- un funcionamiento descentralizado,
- mecanismos consensuales que permiten asociar intereses divergentes,
- una confianza distribuida mediante la supresión del tercero de confianza único.

Nuevas oportunidades surgirán en una nueva economía de la distribución basada en las redes sociales 2.0, donde humanos y objetos conectados interactuarán de forma indiferenciada. La *blockchain* nos permite crear «anclas» entre el mundo físico y el mundo virtual. Así, una operación o transacción en el mundo real puede tener su contraparte en el mundo digital.

Incluso si la *blockchain* no responde a todas las problemáticas, este tipo de solución es muy relevante en campos donde la confianza, transparencia y trazabilidad son indispensables. Sin embargo, no hay que pasar por alto los puntos débiles de la *blockchain* (en particular, la verificación de la autenticidad de los datos almacenados o la verificación de la legitimidad de una operación «no electrónica».

3 - Los *smart contracts* y los oráculos

La regulación de los *smart contracts* y los *smart contracts* de los reguladores

Catherine Barreau, Profesora de la Facultad de Derecho y Ciencias Políticas de la Universidad de Rennes 1, IODE UMR CNRS 6262, Universidad Bretagne-Loire

Tarde o temprano, toda innovación tecnológica debe enfrentarse a la prueba del derecho. La necesidad de regulación se expresa tanto por parte de los usuarios de la innovación, que se benefician de ella, como por aquellos que pueden ser víctimas de ella. De esta forma, las cadenas de bloques han tomado discretamente su lugar en el entorno legal, en el ámbito de la financiación de las empresas. Los *smart contracts*, cuyos casos de uso aún son limitados, deberán dentro de poco hacerles compañía, ya que la complejidad de la herramienta requiere un marco jurídico seguro para su desarrollo. Reglamentar este nuevo objeto requiere determinar su naturaleza para establecer sus usos. Aunque éstos sean principalmente privados, su uso público, por parte de una autoridad de regulación, puede también considerarse.

Aspectos jurídicos de los *Smart contracts*

Eric Barbry, Abogado, Director del Centro de Derecho digital del Gabinete Alain Bensoussan Avocats Lexing

Los *smart contracts* (contratos inteligentes) no son una nueva forma de contrato que se opone a los contratos idiotas...

En realidad, los *smarts contracts* ni siquiera son contratos...

Los *smart contracts* son una forma de codificar un contrato y hacer que su aplicación sea automática, por lo tanto más fácil, rápida y segura.

Los *smart contracts* están basados en la tecnología de la *blockchain*. Esta tecnología interesa a muchos sectores: las finanzas, la música, los intermediarios o los secuestres.

Como todas las técnicas, los *smart contracts* ofrecen muchas ventajas, pero también presentan muchos interrogantes, entre los cuales: ¿Cómo se garantiza su seguridad? ¿Qué pasa con los errores de programación?

La aplicación de la *blockchain* y de los *smart contracts* por parte de las industrias culturales

Jérôme Pons, Consultor en tecnologías y estrategias digitales en el ámbito de la cultura y responsable de la normalización de la *blockchain* de Music won't stop

La contractualización es omnipresente en las industrias culturales, especialmente en los sectores del cine, vídeo y de la música grabada. Sin embargo, los contratos no siempre se pueden aplicar o ejecutar, ya sea que se trate de contratos de autor, edición, licencia o de distribución. En realidad, los «mínimos garantizados» pueden llevar a una transferencia «excesiva» de valor hacia los productores y editores, y la falta de metadatos jurídicos puede afectar la remuneración de los derechohabientes (como los artistas intérpretes). En este contexto, ¿es utópico imaginar una programación y ejecución automáticas de los contratos, que llevaría a una repartición «equitativa» del valor entre creadores, productores, editores, distribuidores, operadores y consumidores de contenidos digitales y una remuneración de los derechohabientes que refleje el consumo basado en el número de descargas o escuchas? La tecnología *blockchain* responde en cierta medida a esta pregunta.

El oráculo *hardware*, la capa de confianza entre las *blockchains* y el mundo físico

Vanessa Rabesandratana, *Customer Success Manager*, Ledger, y **Nicolas Bacca**, *Chief Technical Officer*, Ledger

Las aplicaciones *blockchain* evolucionan en su propio entorno totalmente virtual que por naturaleza está completamente separado del mundo real. Los *smart contracts*, aplicaciones descentralizadas y otras monedas virtuales tienen una influencia limitada sobre el mundo concreto que nos rodea. Ni siquiera se puede hablar de ortogonalidad ya que estos universos existen en planos que no se superponen nunca.

Cada uno de los casos de uso nos remite a esta problemática: ¿cómo pueden las aplicaciones relacionadas con la *blockchain* interactuar de manera eficiente y segura con el mundo real, y cómo los *smart contracts* pueden alimentarse de datos externos, todo ello, de forma segura y eficaz?

Esta pregunta surgió naturalmente desde el comienzo de esta tecnología y hubo que diseñar las herramientas e interfaces adaptadas. La plataforma de confianza que permite establecer vínculos entre el mundo real y la *blockchain* tiene un nombre: oráculo.

4 - Oportunidades y retos

Por qué se interesa la normalización en la *blockchain*

Olivier Peyrat, Director General de la Asociación Francesa de Normalización (Afnor), y **Jean-François Legendre**, Responsable de desarrollo de la Afnor

La *blockchain* se refiere a un conjunto de tecnologías. Su potencial de desarrollo es enorme, con numerosos casos de uso previstos, algunos de los cuales ya están en fase de despliegue. El impacto potencial de la *blockchain* es revolucionario y sin duda estratégico para muchos sectores. Sin embargo, la *blockchain* deberá llegar a un primer nivel de madurez, lo que implica el desarrollo de normas con el fin de aportar la confianza necesaria en algunos aspectos de los procesos puestos en marcha.

Seguridad e inseguridad de la *blockchain* y de los *smart contracts*

Jean-Pierre Flori, Experto en criptografía de la Agencia Nacional de seguridad de los sistemas de información (ANSSI)

La seguridad de muchas aplicaciones que utilizan las *blockchains* se basa no sólo en la forma en que se construyen las *blockchains* subyacentes, sino también en las particularidades de la aplicación construida con ayuda

de los datos almacenados en estas *blockchains*, así como el comportamiento de las entidades que participan en la expansión de la *blockchain*. En este artículo, se analizan estos niveles de seguridad, ilustrándolos gracias a dos aplicaciones emblemáticas de las *blockchains*: la criptomoneda bitcoin y el ordenador-mundo Ethereum.

La o las *blockchain(s)*, una respuesta tecnológica a la crisis de confianza

Arnaud Manas, Ingeniero, Doctor en economía e historia, investigador asociado de la Universidad de París I - Sorbonne (IDHES), y **Yoram Bosc-Haddad**, especialista de la gobernanza de las iniciativas emergentes y de pilotaje económico

En su forma canónica, la *blockchain* es un rechazo de los terceros de confianza. Esta tecnología se basa en una posición ideológica que no está exenta de populismo. Este rechazo de las instituciones establecidas se explica en parte por la crisis de confianza que atraviesan las sociedades modernas. El solucionismo tecnológico que desea establecer la confianza mediante algoritmos, sin anclaje social o jurídico, es ilusorio. Teniendo en cuenta los costes y riesgos, el uso de la *blockchain* canónica (sin terceros de confianza) presenta poco interés con excepción de un número de campos limitado. Por el contrario, la aplicación de las tecnologías *blockchain* por parte de instituciones de confianza, dentro de un marco jurídico y social, parece tener un futuro brillante. Pero sólo una vigilancia activa permitirá que sus agentes se beneficien plenamente de ella.

Una nueva herramienta digital para la seguridad de las *supply chains*, la *blockchain*

Matthieu Hug, *Serial Entrepreneur*, cofundador y CEO de Tilkal

Los registros digitales distribuidos (*blockchains*) prometen reinventar la confianza, haciendo posibles sistemas de notariado descentralizados y sin intermediarios. Su aplicación a la industria financiera, la cual se ha estudiado y comentado ampliamente, podría modificar nuestros sistemas de intercambios basados en terceros de confianza.

Por su parte, otras aplicaciones de estas tecnologías desean no solamente sustituir los mecanismos de confianza existentes, sino también crear confianza allí donde ésta hace falta. Una aplicación con un interés sanitario principal es la garantía de la trazabilidad de los productos a todo lo largo de la cadena, desde el fabricante hasta el consumidor: en primer lugar, para proporcionar al consumidor la transparencia que reclama sobre lo que se consume, y la conformidad, que quiere evaluar, según sus criterios de salud o ética. A continuación, para luchar contra el increíble crecimiento de todo tipo de falsificaciones, que afectan a todas las industrias, desde la industria farmacéutica hasta los alimentos para lactantes o las piezas para automóviles.

Smart business networks: The evolution

Louis-François Pau, Rotterdam School of Management and Copenhagen Business School

The intelligence of an information network is augmented by its functionality (its ability to distribute, store, assemble, or modify information). Transmission networks are technically complex, but business-wise they are “dumb” pipes that transport information without enhancing it. An information network augmented by formalized business relationships can be “smart”; it can improve the utility of information in multiple ways (that is synonymous with creating economic value).

Conversely, a lone transaction between two business partners rarely stands isolated, especially in an electronic commerce context, but the economic value accrues already then for both partners. New transactions can be created with the same or other partners, by cascading whole or parts of the same initial transaction, thus building a network of business relations which develops over time.

To address the two above paradigms, has been defined the concept of “Smart Business Network” (SBN).

*El dossier ha sido coordinado por **Jean-Pierre Dardayrol***

BACCA Nicolas

Nicolas Bacca est *Chief Technical Officer* de Ledger.

BARBRY Éric


D.R

Avocat à la Cour d'appel de Paris, Éric Barbry est directeur du pôle Droit numérique du cabinet Alain Bensoussan Avocats - Lexing. Il intervient en matière de conseil, de contrats et de contentieux dans les domaines du droit de l'Internet, des plateformes, des données personnelles, du *marketing* digital, de la dématérialisation et de la sécurité des systèmes d'information.
Il a été nommé membre du Conseil supérieur de la propriété littéraire et artistique, par arrêté du ministre de la Culture et de la Communication du 30 septembre 2015, et est également chargé d'enseignement en droit des technologies de l'information et de la communication à Télécom ParisTech.
Il préside la Commission juridique de l'ACSEL, l'association de l'économie numérique et de la transformation digitale.
Il est coauteur de plusieurs articles publiés dans des revues professionnelles de la presse spécialisée et a contribué à la rédaction de plusieurs ouvrages, dont *Droit de l'informatique, télécoms et Internet* (Éditions Francis Lefebvre, 5ème édition 2012) et *Code de la sécurité informatique et télécom* (Éditions Larcier, mai 2016).

BARREAU Catherine

Catherine Barreau est professeur à la Faculté de droit et de science politique de l'Université de Rennes 1, où elle dirige le magistère « juriste d'affaires franco-britannique ». Membre de l'Institut Ouest Droit Europe (UMR CNRS 6262), elle est membre de l'équipe de droit européen et s'intéresse aux questions de politique européenne en matière de concurrence, de protection des consommateurs et de droit du numérique. Ses travaux portent sur la reprise de l'acquis communautaire en matière de droit de la consommation (Pologne, France), sur l'articulation entre le droit européen et les droits nationaux de la concurrence (compétences comparées des Autorités nationales compétentes en la matière et de la Commission). Elle a aussi publié plusieurs articles en droit de l'entreprise et sur la marchandisation des données personnelles. Elle est vice-présidente de l'Université numérique juridique francophone (U.N.J.F.) et est en charge du Conseil pédagogique et scientifique de cette même université.

BEAUDEMOULIN Nathalie

Diplômée de Sciences-Po Paris, Nathalie Beaudemoulin est coordinatrice du pôle Fintech Innovation de l'Autorité de Contrôle prudentiel et de Résolution (ACPR). Elle justifie de vingt ans d'expérience dans la supervision bancaire. Elle a été notamment directrice adjointe des agréments et de la réglementation à l'ACPR. Elle préside le groupe de


D.R

travail de l'Autorité bancaire européenne sur l'innovation financière et contribue aux travaux du Comité de Bâle et du Forum de stabilité financière consacré à cette même question.

BEDOIN Thierry


D.R

Thierry Bedoin est diplômé de l'École centrale de Lyon et de Supélec. Il travaille à la Banque de France depuis 1983. Après avoir dirigé la production informatique de la Banque, il a été nommé directeur de l'organisation du système d'information. Depuis octobre 2016, il est *chief digital officer* (directeur de la transformation digitale). Son rôle est d'impulser et d'animer la transformation digitale de la Banque de France, d'en élaborer la stratégie digitale, de coordonner la mise en œuvre des actions digitales, d'accompagner les métiers dans leur transformation et de développer la démarche d'innovation en construisant une relation collaborative avec les acteurs innovants au sein du Laboratoire Banque de France.

BERBAIN Côme

Ingénieur des mines et docteur en cryptologie, Côme Berbain est sous-directeur adjoint Expertise à l'Agence nationale de la sécurité des systèmes d'information (ANSSI).
En 2004, il débute sa carrière chez Orange en R&D, où il s'occupe de cryptographie et contribue à la normalisation de la 4G. En 2008, il rejoint le ministère de la Défense en qualité d'expert en sécurité, avant d'y exercer des responsabilités managériales. En 2012, il intègre la PME Trusted Logic, qui est spécialisée dans la fabrication de cartes à puce, en tant que responsable de la sécurité. En 2014, il revient au ministère de la Défense en tant que conseiller en stratégie chargé d'opérer un rapprochement entre deux services. En 2015, il s'intéresse à la transformation numérique du secteur de l'assurance avant d'intégrer l'ANSSI, où il se voit confier notamment une mission d'optimisation numérique de l'Agence.
Ses principaux sujets d'intérêt portent sur la sécurité du numérique et la transformation numérique des organisations.

BORTZMEYER Stéphane

Stéphane Bortzmeyer est ingénieur à la direction Système d'information et opérations de l'AFNIC (https://www.afnic.fr/), où il est en charge notamment de la veille technologique, ce qui l'amène tout naturellement à s'intéresser à la chaîne de blocs : il a à ce titre conçu le tutoriel *blockchain* ayant servi de support à la Journée du Conseil scienti-


D.R

fique de l'AFNIC (https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/10075/show/jcsa16-retour-sur-la-journee-du-conseil-scientifique-de-l-afnic-2016.html) organisée en 2016. Il a également contribué à l'élaboration du dossier thématique de l'AFNIC (https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/10306/show/l-afnic-publie-un-nouveau-dossier-thematique-sur-la-chaine-de-blocs-blockchain.html) consacré à ce sujet. Il réserve dès qu'il le peut un peu de son temps à son ordinateur personnel qui constitue un nœud des technologies Bitcoin, Namecoin et Ethereum. On peut le joindre par courrier électronique à l'adresse suivante : bortzmeyer@nic.fr, ou sur le réseau social Mastodon sous l'adresse bortzmeyer@mastodon.gougere.fr

BOSC-HADDAD Yoram

Yoram Bosc-Haddad est statisticien économiste (ENSAE) et docteur en informatique (Paris-Sud Orsay). Il est directeur associé d'Ylios, société de conseil en gestion des affaires. Il était précédemment *lean officer* au sein du Groupe Capgemini, et avait auparavant exercé pendant quinze ans des activités de conseil en management et avait consacré six années à la transformation engagée dans la sidérurgie. Il est un spécialiste de la gouvernance des initiatives émergentes et du pilotage économique : il a à ce titre dirigé de nombreuses missions de conseil auprès de directions générales et financières dans les secteurs du numérique, de la pharmacie, de l'industrie, de l'énergie et des services financiers.
Il est également administrateur d'ESIEA, qui est une grande école d'ingénieurs en informatique et membre du comité d'honneur des Glénans et d'Ashoka Support Network.

CARTON Malo

Malo Carton est diplômé de l'École polytechnique (promotion 2008) et ingénieur du corps des Mines. Il a débuté sa carrière dans l'administration à la direction générale du Trésor, au sein du bureau « Épargne et marchés financiers », où il a travaillé sur des sujets touchant à la réglementation de l'organisation et du fonctionnement des marchés secondaires d'instruments financiers. À cette occasion, il a contribué aux travaux relatifs à la définition d'un cadre réglementaire adapté à la *blockchain* France consacrée aux minibons et aux titres financiers. Il travaille actuellement à l'Agence des participations de l'État.

CIAVALDINI Pierre-Alexis

CEO de MakerNet, programmeur et inventeur, Pierre-Alexis Ciavaldini est étudiant-entrepreneur à l'École 42. De la création d'imprimantes 3D pour les Beaux-Arts à la conception d'objets connectés, c'est tout naturellement qu'il rejoint le mouvement Maker.
Il est aujourd'hui intervenant spécialiste de la technologie


D.R

blockchain et co-fondateur du BlockFest, un festival pédagogique consacré aux *blockchains*. Convaincu de l'importance de la culture *maker* en tant que moyen citoyen pour garder un certain contrôle sur la technologie, il cherche à mettre en place de nouveaux paradigmes de gestion distribuée, d'éducation continue et de liberté dans le travail. C'est dans cette optique qu'il crée MakerNet au sein du mouvement FabCity, en 2015. Il rejoint AllMade Consulting aux cotés de Jean-Pierre Seck après avoir découvert le projet de gestion des droits d'auteur AllMedia lors de la première édition du BlockFest organisée en 2016. Il repense ainsi le système des droits d'auteur en apportant son expertise aux industries créatives.

COLLOMB Alexis

Alexis Collomb est titulaire de la chaire de finance du Conservatoire national des Arts et Métiers (CNAM), où il dirige également le département Économie Finance Assurance Banque (EFAB). Il a fondé le SciChain Lab, qui se focalise sur les *blockchains* et autres registres distribués. Il est co-directeur scientifique du projet *Blockchain Perspectives Joint Research Initiative* réalisé en partenariat avec BNP Paribas.

DARDAYROL Jean-Pierre


D.R

Ingénieur général des mines, Jean-Pierre Dardayrol est président du Comité de rédaction de la nouvelle série des *Annales des Mines* intitulée *Les enjeux numériques*. Le premier numéro de cette nouvelle série, dont la parution devrait intervenir en mars 2018, sera consacré à l'Intelligence artificielle.

DSAINBAYONNE Jurgen

Juriste en droit des affaires, une formation qu'il a complétée par des études en économie et en analyse financière, Jurgen Dsainbayonne a rapidement délaissé le droit pour se tourner vers le *Web* en tant qu'autodidacte, renouant ainsi avec sa passion initiale pour les nouvelles technologies et les mathématiques.
Travaillant sur des projets digitaux, en tant que consultant tout d'abord, puis de *free lance* SEO, Jurgen Dsainbayonne s'est très tôt intéressé au phénomène bitcoin et à la technologie sous-jacente, la *blockchain*. Amoureux d'art et très attiré par ce milieu, il a très vite réalisé le potentiel que cette innovation majeure pouvait représenter pour le marché de l'art.
C'est ainsi qu'il s'est lancé dans l'aventure *start-up* en fondant Seezart, dont l'ambition est d'être le garant d'un marché de l'art en pleine mutation digitale, et ce en implé-

mentant la technologie *blockchain* de manière à développer une nouvelle solution de certification des œuvres d'art et d'attestation de leur provenance qui soit infalsifiable.

FLORI Jean-Pierre

Jean-Pierre Flori est diplômé de l'École polytechnique et est titulaire d'un doctorat en informatique. Depuis octobre 2011, il exerce en qualité d'expert en cryptographie au sein de l'Agence nationale de la sécurité des systèmes d'information.

GENESTIER Philippe


D.R

Docteur en microélectronique, Philippe Genestier travaille depuis 1999 au sein d'Orange Labs, successivement en qualité de responsable d'équipe, puis de chef de projet. Ses activités actuelles englobent la responsabilité des activités de recherche d'Orange dans le domaine de la santé, lesquelles recouvrent notamment l'interopérabilité dans la collecte de données de santé. Dans le cadre de ses recherches, il a initié plusieurs projets mettant en œuvre la *blockchain* dans les domaines IoT et de l'e-santé. Il est l'auteur de plusieurs publications sur les différents usages de cette technologie. Il assure également la responsabilité de l'encadrement de travaux de thèse.

HUG Matthieu

Matthieu Hug est un serial entrepreneur, co-fondateur et CEO de Tilkal, une plateforme d'identité numérique pour les produits et les biens. Passionné par les technologies numériques, Matthieu Hug siège, en parallèle de ses activités, au sein des conseils d'administration de plusieurs *start-ups* innovantes.

Entre 2007 et 2016, Matthieu Hug co-fonde et dirige *RunMyProcess*, une plateforme « *cloud* » unique qui aide des centaines d'entreprises à surmonter les obstacles technologiques qu'elles rencontrent dans leur transformation numérique. *RunMyProcess* est acquise en 2013 par le groupe Fujitsu.

Ingénieur Supélec de formation (promo 97) et détenteur d'un Master of Science du prestigieux Georgia Institute of Technology, Matthieu Hug a débuté sa vie professionnelle dans le conseil en matière de numérique.

JÉRÉMIE Pierre


D.R

Pierre Jérémie est diplômé de l'École polytechnique (promotion 2008) et ingénieur du corps des mines. Il est actuellement en poste à la direction régionale et interdépartementale de l'environnement et de l'énergie en tant que chef du service de prévention des risques et des nuisances.

LAURENT Xavier

Diplômé de l'IUP MIAGE – IFSIC et titulaire d'un Master 1 *Accounting & Control of Management* de l'Université Laval (Québec), Xavier Laurent, après une expérience de deux ans au NYSE Euronext, travaille pendant sept ans au sein du groupe Crédit Agricole où il est successivement *PMO Compliance IT-team leader,* responsable de la PMO *Risk & Compliance IT*, responsable du pilotage des projets IT et membre de l'équipe Innovation transverse et est à ce titre responsable de la communauté *blockchain*.

LEGENDRE Jean-François


D.R

Responsable Développement de l'Association française de normalisation, Jean-François Legendre est le rapporteur du Comité stratégique de l'Afnor sur la normalisation du secteur de l'information et de la communication numérique, un Comité qui a anticipé et instruit les besoins normatifs pour la *Blockchain*.

Jean-François Legendre est par ailleurs membre de plusieurs groupes de coordination stratégique existant au sein de diverses instances internationales, notamment le Comité européen de normalisation (CEN) et l'Institut européen de standardisation des télécommunications (ETSI).

LÉGER Lucas


D.R

Lucas Léger est chercheur et doctorant au CNAM, où il réalise une thèse sur la *blockchain* et les *smart contracts*. Il s'intéresse plus particulièrement aux problématiques d'automatisation et d'incomplétude de ces derniers.

LETONDEUR Loïc


D.R

Ingénieur de l'École polytechnique de Grenoble, Loïc Letondeur est titulaire d'un doctorat en informatique (2014) de l'Université Joseph Fourier, ses travaux de thèse ont porté sur l'intelligence artificielle des systèmes autonomiques en environnement de *Cloud computing*.

Après avoir travaillé pendant un an au sein d'une filiale du groupe japonais Fujitsu en tant qu'ingénieur en recherche et développement, il rejoint en 2016 Orange Labs pour y poursuivre ses travaux. Depuis lors, il s'implique fortement dans des problématiques de gestion autonomique du cycle de vie des applications massivement distribuées en environnement de *Fog Computing* et de l'intelligence des

applications dévolues à l'internet des objets par *Complex Event Processing*. Ses travaux l'ont ainsi amené à étudier la technologie *Blockchain* et à l'utilisation de celle-ci en environnements à la fois contraints, conflictuels et massivement distribués.
Auteur de plusieurs publications et impliqué dans l'encadrement de travaux de thèse, il a également participé à de nombreux projets collaboratifs.

MANAS Arnaud

Arnaud Manas est ingénieur, docteur en économie et en histoire. Il est chercheur associé à l'Université Paris I-Sorbonne (IDHES). Ses travaux portent principalement sur l'histoire des monnaies françaises et sur celle de la Banque de France. Il a été le modérateur du cycle de conférences « Monnaies virtuelles et monnaies locales, quels enjeux ? » organisé par la Bibliothèque nationale de France en mars 2017. Il est aussi l'auteur de deux ouvrages récents : *L'Or de Vichy* (Éditions Vendémiaire, 2016) et *Zweig & la Souterraine de la Banque de France* (Artélia Éditions, 2016). En 2015, il reçoit le *Highlight* de l'*European Journal of Physics*.

MARIN-DAGANNAUD Gautier


D.R

Gautier Marin-Dagannaud est élève-ingénieur à Télécom Paristech et est étudiant en master à l'École polytechnique. Il travaille actuellement chez Ledgys, une *start-up* française développant des solutions *blockchain*. Il est également rédacteur chez Ethereum France et co-fondateur de l'association Asseth.

PAU Louis-François

Louis-François Pau (email: lpau@nypost.dk) is Professor at Rotterdam School of Management, Erasmus University, in the field of High tech business , and Adjunct Professor in Mobile business at the Copenhagen business school, besides other governmental or industrial assignments.
He was 1995- 2008 Chief Technology Officer (Executive CTO) of L.M. Ericsson's Network Systems division with worldwide responsibilities , which he joined from a prior position (1990-1995) as CTO for Digital Equipment Europe / Hewlett Packard Europe with oversight over engineering staff in Europe and Asia. In this CTO role, he oversaw the product developments and technology engagements in infrastructure, services and tools.
He was earlier (or in parallel) on the faculties of Danish Technical University, Ecole Nationale Supérieure des Télécommunications (Paris), M.I.T, University of Tokyo, and has been lecturing also at: University of Maryland, University of Mannheim, University of Regensburg, George Washington University, Institut Aéronautique et de l'Espace, University of Brasov.
He is on the IEEE European Policy Committee, which interacts with the Commission on technology policy issues on behalf of IEEE.
He is a Fellow of IEEE (USA), BCS (UK), and JSPS (Japan). He holds an MSc from ENS Aéronautique et Espace (Paris) , MBA from Institut d'études politiques, Dr. Ing. from Univ. Paris 9 , and DSc from Univ. Paris 6, besides executive education at IMD & INSEAD.
He has over 400 publications (h-index: 19, g-index: 36, over 3000 citations, & SSRN rank: in top 1,5 %).

PAVEL Ilarion


D.R

Docteur en physique, ingénieur en chef des mines, Ilarion Pavel travaille au sein du Conseil général de l'Économie, de l'Industrie, de l'Énergie et des Technologies et du Laboratoire de physique théorique de l'École normale supérieure, dans le domaine de la physique des particules élémentaires et interactions fondamentales.
Il a été ingénieur de recherche chez Thomson-CSF et a effectué un séjour post-doctoral à Caltech (Californie). Pendant trois ans, il a travaillé à la délégation régionale de la recherche et de l'innovation de l'Île-de-France, dans le domaine de l'innovation et du transfert de technologie, puis il a été en charge durant cinq ans du Réseau national de recherche en télécommunication, au ministère de la Recherche. Par la suite, au sein de ce même ministère, il a été conseiller scientifique en nanotechnologies.

PEYRAT Olivier


D.R

Olivier Peyrat est directeur général d'AFNOR (Association française de normalisation).
Ancien élève de l'École polytechnique, ingénieur en chef au corps des mines, Olivier Peyrat est administrateur du Comité européen de normalisation (CEN) et administrateur de l'Organisation internationale de normalisation (ISO). Il a été également vice-président Finances de l'ISO de 2013 à 2016. Il est par ailleurs administrateur et membre du bureau du Groupe des industries métallurgiques (GIM).
Olivier Peyrat a également présidé diverses commissions ou groupes de normalisation aux plans national, européen et international, ainsi que le CASCO (*Conformity Assessment Committee*), le Comité de l'ISO chargé de la politique ISO et de l'élaboration des normes internationales dans le domaine de l'évaluation de conformité : essais, certification, inspection, accréditation, etc. Il est également, depuis 2016, membre du Comité d'experts normalisation auprès du gouvernement chinois.

PONS Jérôme

Jérôme Pons débute sa carrière chez Orange, étant successivement délégué à la normalisation 3GPP, chef

de projet Orange Media Player (*Music Podcasts*), chef de projet *marketing Web TV* (OCS), puis de responsable du programme de tests d'interopérabilité (IOT). En 2011, il fonde la société de production de spectacles Music won't stop, qui se diversifie en 2013 en développant une activité de conseil en matière de technologies et de stratégies numériques. Spécialiste des enjeux associés à la transformation numérique des secteurs de la culture (financement de la culture, partage de la valeur, gestion de droits basée sur les métadonnées, protection de la propriété intellectuelle), il a développé une solide expertise dans la modélisation et la gestion des données. Depuis 2016, il se consacre à la normalisation internationale de la *blockchain* et anime le groupe de travail « Architecture et modélisation » de l'Afnor. Il participe également à plusieurs groupes d'étude (dont celui consacré aux *smart contracts*) de l'ISO/TC 307.

PROLA Alain

D.R

Alain Prola est concepteur/développeur d'applications sur plateforme Android. Il a co-développé un connecteur Continua dans une chaîne de collecte de données médicales. Précédemment il a développé plusieurs applications mobiles pour les pays émergents. Avant cela, il a travaillé pendant dix ans dans la recherche en microélectronique.

RABESANDRATANA Vanessa

Vanessa Rabesandratana est *Customer Success Manager* chez Ledger

ROBERT Arnaud

Arnaud Robert est directeur juridique du groupe Hachette Livre depuis 2011.
Il est président du Centre français d'exploitation du droit de copie (CFC) depuis 2014 et président de la mission juridique du Syndicat national de l'édition (SNE) depuis 2016.
Il est chargé d'enseignement en droit des médias à l'Institut national de l'audiovisuel (INA).
De 1998 à 2001, il a été avocat au barreau de Paris exerçant au sein du Cabinet Fourgoux & Associés.
Il a ensuite travaillé au sein du groupe de médias NRJ Group, en tant que directeur juridique adjoint du groupe, de 2001 à 2011.
Arnaud Robert est titulaire du CAPA (barreau de Paris), du DESS de droit européen des affaires - Université Paris II Panthéon-Assas (L. Vogel) et est diplômé du *Trinity College of Dublin*.

ROSET Alain

Après des études à l'École polytechnique (75) et à Télécom Paris Tech (80), Alain Roset débute sa carrière en travaillant à la conception de l'architecture du premier microprocesseur européen, avant de participer au financement de projets d'électronique au ministère de l'Industrie. Après avoir participé à l'organisation des Jeux Olympiques d'Albertville où il était en charge des télécommunications, il rejoint La Poste pour y exercer des responsabilités opérationnelles au niveau régional, puis au niveau national, au sein de la division Courrier. Par la suite il travaille au développement des technologies de rupture dans les marchés du courrier et des colis, il teste et développe de nouvelles activités pour les facteurs, puis rejoint, en 2014, la nouvelle division numérique qui vient juste d'être créée, il a à y connaître les nouveaux défis numériques que posent les échanges sécurisés de documents, le développement de la technologie *Blockchain*, la traçabilité et l'Internet des objets.

ROSSIGNOL Éric

Ancien élève de l'École normale supérieure de Lyon et de l'École nationale des Ponts et Chaussées, il travaille pendant cinq ans sur la structuration de produits dérivés sur actions au sein du groupe Caisse des Dépôts, puis, pendant une douzaine d'années, au sein du département Titrisation du groupe Crédit Agricole. Il est actuellement en charge de l'analyse quantitative et du laboratoire d'innovation du département Titrisation, au sein duquel ont été conçus deux prototypes basés sur la *blockchain* Ethereum.

SOK Klara

D.R

Klara Sok est chercheuse et doctorante au CNAM, où elle réalise une thèse sur la *blockchain* et la question de l'intermédiation. Elle s'intéresse tout particulièrement aux changements sociologiques et organisationnels générés par cette technologie en tant qu'alternative organisationnelle aux structures existantes.

STEPHAN François

D.R

François Stephan est directeur général adjoint en charge du développement et de l'international de l'Institut de recherche technologique SystemX, un Institut dédié à l'ingénierie numérique des systèmes complexes.
Ingénieur diplômé de l'École polytechnique (86) et de Télécom ParisTech (91), il justifie de plus de vingt-cinq ans d'expérience professionnelle dans le secteur des technologies de l'information, au sein duquel il a assuré des fonctions de

pilotage de projets, de direction produit, de conseil, de direction technique et d'animation d'écosystèmes.
Il est co-auteur avec Jean-Pierre Briffaut de l'ouvrage *Cloud Computing : évolution technologique, révolution des usages,* publié en mai 2013 aux Éditions Hermes Science - Lavoisier.

TEMERSON Jean-Marc


D.R

Jean-Marc Temerson est ingénieur en chef des mines diplômé de l'École polytechnique (X 75) et de l'École nationale supérieure des télécommunications (ENST 80). Titulaire d'un DEA en microélectronique, il a débuté sa carrière au CENT, puis a rejoint Orange Labs, où il a été successivement ingénieur de recherche, responsable d'équipe et responsable de projet.
Débutant celle-ci dans la microélectronique silicium, où il a piloté de nombreux projets européens, et la poursuivant en prospective de services, il s'est ensuite investi dans le domaine des télécommunications sous l'angle du développement durable, puis, dans le cadre de projets européens, il a travaillé à la conception de réseaux mobiles reconfigurables, avant de s'intéresser à la télémédecine, plus particulièrement à la télé-imagerie médicale en anatomocytopathologie (projet collaboratif national).
Depuis 2015, il s'implique dans la télécollecte de données de santé issues des objets connectés. Plus récemment, son travail s'est centré sur l'intérêt que revêtent certains mécanismes de la *Blockchain* en matière de gestion du consentement des patients à l'accès à leurs données médicales.
Auteur de nombreuses publications et responsable d'encadrement de travaux de thèse, il est retraité d'Orange depuis mars 2017.

WAELBROECK Patrick

Patrick Waelbroeck est titulaire d'une thèse en économie de l'Université de Paris 1 Panthéon-Sorbonne et est professeur d'économie industrielle et d'économétrie à Télécom ParisTech. Ses travaux portent sur l'économie de l'innovation, l'économie de la propriété intellectuelle, l'économie de l'Internet et des données personnelles. Il est membre du bureau de l'association EPIP (*European Policy for Intellectual Property*), dont il a été le président en 2013-2014. Il est cofondateur de la chaire « Valeurs et politiques des informations personnelles » de l'Institut Mines-Télécom qui aborde les problèmes des données personnelles et du *Big data* sous différents angles : juridique, économique, technique et philosophique. Patrick Waelbroeck enseigne l'économie de l'Internet et des données dans le mastère spécialisé *Big data* de Télécom ParisTech, ainsi qu'aux ingénieurs élèves du corps des mines. Il est area editor de la revue *Annals of Telecommunications* et membre du comité éditorial du *Journal of Cultural Economics*.

WAIGNIER Christophe


D.R

Christophe Waignier pilote les domaines Finances, Ressources humaines, Informatique, Stratégie et Développement de la Sacem.
Il est également président de FastTrack, qui regroupe les treize sociétés de gestion de droits d'auteur les plus importantes du monde. Ce réseau développe des solutions devant permettre un meilleur partage des métadonnées musicales entre les acteurs du secteur considéré.
Diplômé de l'Institut d'études politiques de Paris, Christophe Waignier débute sa carrière en tant qu'auditeur chez Price Waterhouse, puis il exerce pendant dix ans en qualité de directeur administratif et financier dans l'industrie audiovisuelle. En 1995, il rejoint BMG Entertainment en tant que directeur financier, puis est nommé, en 1999, senior vice-président Finance et opérations Europe. En 2003, Christophe Waignier devient directeur général de BMG France, avant d'occuper les mêmes fonctions chez SonyBMG France. Entre 2008 et 2012, avant de rejoindre la Sacem, il a travaillé en tant que consultant dans le domaine de la stratégie de transformation des entreprises.

WARZÉE Didier


D.R

Ingénieur des mines, diplômé de l'École nationale de la statistique et de l'administration économique et actuaire certifié de l'Institut des actuaires, Didier Warzée est expert au sein du Pôle Fintech Innovation de l'ACPR. Après avoir débuté sa carrière en qualité d'actuaire, il développe une expertise en *risk management,* avant d'encadrer une équipe de *scoring* au sein d'une société de financement. En 2009, il rejoint l'ACPR pour intégrer des équipes de contrôle des organismes d'assurance. De 2013 à juin 2016, il est nommé adjoint au sein du service des organismes d'assurance, où il est en charge des agréments. Il fait depuis lors partie de l'équipe constituante du pôle Fintech-Innovation de l'ACPR.

ZOUARHI Sajida


D.R

Sajida Zouarhi est ingénieure et doctorante en informatique et réseaux depuis 2014 chez Orange Labs et au LIG (Laboratoire d'informatique de Grenoble INP). Ses travaux de recherche portent sur la qualité de service de systèmes complexes et hétérogènes de transmission de données critiques. Elle étudie également les mécanismes des *blockchains*.

Cofondatrice de l'association française Chaintech, elle crée en 2015 la communauté Magmateek, constituée autour d'un *meetup blockchain* à Grenoble, celle-ci rassemble plus de 330 personnes qui s'intéressent à différents sujets (impacts et défis de la *blockchain* et projets de demain).
Elle a participé à la création du BlockFest, le premier festival pédagogique des *blockchains.* La première édition de ce festival a été organisée par l'École 42 en juin 2016, elle a été suivie depuis lors de plusieurs autres éditions (Rennes, Grenoble, etc.).

Elle est également l'auteure de plusieurs publications en lien avec la *blockchain* et notamment d'un outil de réflexion, le *Blockchain Canvas,* qui est utilisé par différents acteurs (Healthcare Data Institute, EDF, Orange, etc.) et dans le cursus scolaire d'élèves ingénieurs (ESILV).
Elle assure depuis 2015 le pilotage du projet Kidner, un projet collaboratif qui vise à réduire le temps d'attente des personnes ayant besoin d'une greffe de rein en augmentant leur chance de trouver un donneur compatible grâce au don croisé (www.kidner-project.com).