LE FORUM ÉCONOMIQUE MONDIAL PRÉTEND QUE D'ICI DIX ANS, 10 % DU PRODUIT INTÉRIEUR BRUT MONDIAL SERA STOCKÉ SUR UNE *BLOCKCHAIN* ET QUE CERTAINS GOUVERNEMENTS S'EN SERVIRONT POUR COLLECTER LES IMPÔTS[1].

LA BLOCKCHAIN, VOUS CONNAISSEZ ?

Plusieurs grandes compagnies d'assurance dans le monde investissent déjà dans la recherche et le développement entourant cette technologie et les concepts qui en découlent, comme la cryptomonnaie et les contrats intelligents. L'objectif : déterminer les applications possibles en assurance de dommages et en expertise en règlement de sinistres. Alors, qu'est-ce que la *blockchain* et quel potentiel recèle-t-elle pour l'industrie ?

Origines de la *blockchain*

Jonathan Hamel, entrepreneur, consultant et spécialiste des technologies mobiles et financières, explique : « La *blockchain* trouve son origine dans la cryptodevise bitcoin, introduite autour de 2008 ou 2009 par un certain Satoshi Nakamoto, dont on ignore toujours l'identité réelle. » Il s'agit en quelque sorte d'un grand registre comptable virtuel dans lequel sont enregistrés les transactions et les soldes des utilisateurs du bitcoin, et dont la mise à jour est effectuée par le réseau lui-même.

Par extension, le terme désigne aujourd'hui un ensemble de réseaux qui reprennent les mêmes principes. On retrouve notamment le réseau Ethereum, « une plateforme de développement d'applications décentralisées (dApp) qui permet d'exécuter des *smart contracts*, ou contrats intelligents », explique M. Hamel. Utilisant la cryptomonnaie ether au lieu du bitcoin, cette chaîne accueille une grande variété de programmes qui sortent du cadre purement monétaire[2] (voir l'encadré à la page 13).

Comment ça marche ?

Afin de comprendre le principe de cette technologie, imaginons qu'une transaction intervient entre deux individus. Dans un modèle classique, on a recours à une autorité centrale tierce, comme une institution bancaire, pour valider la transaction (par exemple pour confirmer la disponibilité des fonds). À l'inverse, la *blockchain* est décentralisée. L'ensemble du réseau va recevoir une notification lui demandant de valider la transaction. Le principe de sécurité part de la prémisse que chaque partie du réseau (nœud) peut avoir été corrompue ou être défectueuse ; tout le réseau s'active donc en même temps pour authentifier la transaction. « Chaque transaction du réseau est enregistrée dans des "blocs" créés en chaîne et reliés entre eux, illustre M. Hamel. Chaque bloc contient un code d'identification unique qui fait référence au bloc qui le précède ainsi qu'à une partie de son contenu[3], et chaque bloc est répliqué dans l'ensemble du réseau, rendant sa suppression ou son piratage quasi impossibles. »

Concrètement, comparons la chaîne à un livre et les blocs à ses pages ; si une page du livre est arrachée et replacée ailleurs dans le livre, la numérotation des autres pages permet d'en constater la disparition ou la modification. Ce n'est qu'une fois authentifiée que la transaction est horodatée puis intégrée à la chaîne, où elle sert de base aux transactions suivantes. Cette vérification nécessite cependant une importante puissance de calcul, qui est obtenue grâce à la participation de « mineurs ». Il s'agit d'individus et d'entreprises qui connectent au réseau leurs ordinateurs équipés d'un logiciel de minage afin de réaliser ces opérations.

►►►

[1] Forum économique mondial. *Deep Shift – Technology Tipping Points and Societal Impact,* n° 310815, septembre 2015, p. 24 et 26. http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.
[2] Blockchain France. « Le lexique de la blockchain », [En ligne]. https://blockchainfrance.net/le-lexique-de-la-blockchain/.
[3] Lexis, Anthony. « A gentle introduction to blockchain technology », [Blogue], 9 septembre 2015. https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/.

Pour en savoir plus sur le bitcoin, consultez aussi le site de l'Autorité des marchés financiers au **www.lautorite.qc.ca/fr/bitcoin-fr-conso.html**.

Andreas M. Antonopoulos, un conférencier spécialisé en matière de bitcoin, aurait déjà comparé cette opération à une grande compétition de sudoku au cours de laquelle les participants recommencent une nouvelle grille dès que quelqu'un trouve la solution et dont la difficulté s'ajuste pour qu'en moyenne, une grille soit résolue toutes les dix minutes[4]. M. Hamel précise que « les mineurs sont rémunérés en cryptomonnaie pour leur apport au réseau. Par exemple, sur le réseau Bitcoin, ils reçoivent 12,5 bitcoins[5] par bloc inscrit dans la chaîne ». Il est cependant impossible de prévoir quel mineur sera mis à contribution. Plus un mineur agit sur le réseau, plus il y a de chances qu'il confirme des blocs dans la chaîne et obtienne en retour sa récompense. Ce faisant, les mineurs ont intérêt à ce que le réseau fonctionne adéquatement, au risque de voir leurs revenus décroître ou disparaître.

M. Hamel croit que « la proposition de valeur de la technologie des blocs réside précisément dans la nature décentralisée de son réseau et dans la vérifiabilité de ses enregistrements sans intermédiaire ». L'origine de la création dans la chaîne peut ainsi être retracée; on prétend même qu'il serait possible de remonter la plus longue chaîne, appelée branche principale, jusqu'à sa création originale par Satoshi Nakamoto et de voir toutes les transactions réalisées ensuite[6]. « C'est comme si un billet de banque possédait toute l'information relative aux transactions précédentes, et ce, jusqu'à sa création à la Banque du Canada », explique M. Hamel.

Application possible en assurance de dommages : les contrats intelligents

Les contrats intelligents, ou autoexécutants, sont apparus avec cette technologie, plus précisément grâce au réseau Ethereum. Ces programmes autonomes exécutent automatiquement les conditions d'un contrat, sans intervention humaine, en s'appuyant sur des sources de données fiables capables de fournir les informations requises[7]. En septembre 2015, pour illustrer le fonctionnement de ce type de contrat, des programmeurs ont réalisé un contrat autoexécutant d'assurance voyage pour indemniser automatiquement des passagers lorsque leur vol d'avion était retardé[8].

Dans ces types de contrats, les conditions peuvent être liées à d'autres blocs de la chaîne; le contrat sera programmé pour vérifier l'existence de ces blocs. Elles peuvent aussi faire référence à une date, à l'expiration d'un délai d'exécution, à un événement ou à la réalisation d'une prestation. Dans ce cas, pour s'exécuter, le contrat aura recours à un « oracle ». Le rôle des oracles est de permettre de valider les conditions d'exécution d'un contrat qui sont extérieures au réseau (par exemple, une base de données d'un aéroport) en exécutant un programme informatique conçu à cette fin.

C'est cette automatisation qui pourrait avoir le plus grand impact en matière d'assurance de dommages et d'expertise en règlement de sinistres. Prenons le cas d'un sinistre automobile touchant, par exemple, un véhicule équipé d'un système télématique. Le boîtier connecté dans la voiture peut envoyer un signal d'accident sous forme de bloc dans la chaîne. La déclaration du sinistre sera ainsi automatiquement vérifiée, datée et enregistrée dans la chaîne globale sécurisée et non modifiable; elle devient ensuite accessible pour l'assureur[9]. Sous réserve que les conditions du contrat aient également été programmées dans la chaîne et qu'un oracle ait donné son aval, l'indemnité pourrait être versée directement à l'assuré. On peut aisément imaginer cette application avec tout objet connecté et, en fait, il existe déjà des applications qui établissent un pont entre l'Internet des objets (les objets connectés) et les chaînes de blocs[10].

L'industrie est-elle prête ?

L'application de cette technologie dans l'industrie se heurte à plusieurs obstacles de taille pour le moment. L'adoption d'un nouveau cadre réglementaire et juridique sera nécessaire pour protéger les consommateurs et les entreprises. Il faudra entre autres déterminer les recours en cas de fraude ou de défaillance d'un contrat intelligent.

De plus, les infrastructures de calcul requises pour un usage massif seraient trop importantes, la capacité actuelle de traitement étant de sept transactions par seconde. Comme toute nouvelle technologie, on devra l'expérimenter avant de la démocratiser, ne serait-ce que pour connaître son potentiel réel.

Sachant toutefois que plusieurs compagnies dans l'industrie mènent actuellement des activités de recherche et de développement autour de cette technologie, une application concrète en assurance de dommages ou en expertise en règlement de sinistres devrait voir le jour plus tôt que tard. ■

[4] Tsukerman, Misha. « The block is hot: A survey of the state of bitcoin regulation and suggestions for the future », *Berkeley Technology Law Journal*, [En ligne], 29 novembre 2015. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2084&context=btlj.

[5] En date du 31 octobre 2016, 1 bitcoin équivaut à plus de 900 $CA. https://bitcoin.fr/Cours-du-bitcoin/.

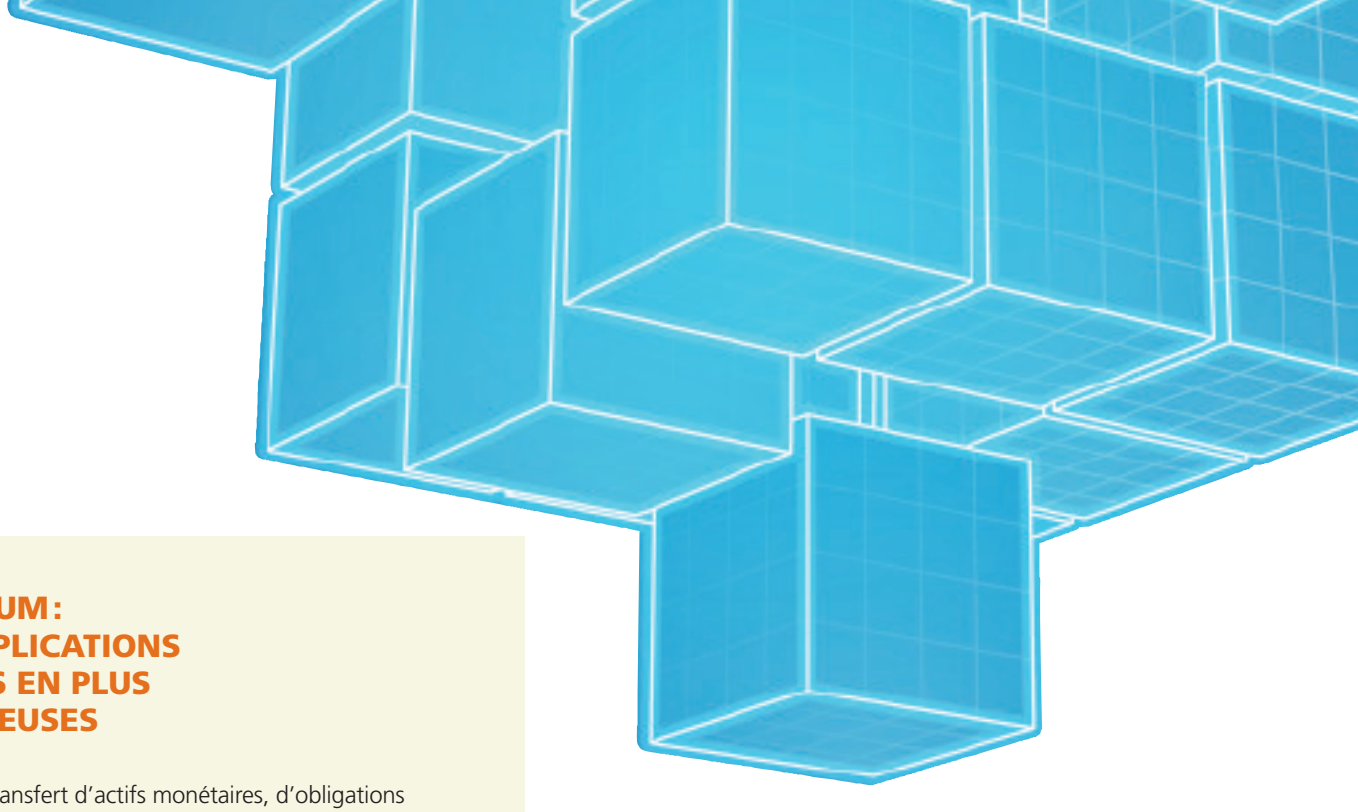
[6] Bitcoin.fr. « Comment la blockchain se constitue-t-elle ? », [En ligne]. https://bitcoin.fr/comment-la-blockchain-se-constitue-t-elle/.

[7] Blockchain France. « Les applications prometteuses des smart contracts », [En ligne]. https://blockchainfrance.net/2016/01/28/applications-smart-contracts/

[8] Blockchain France, *id.*

[9] Lelynx.fr. « Quel potentiel pour la blockchain au sein de l'assurance ? », [En ligne]. https://www.lelynx.fr/assurance-auto/actualites/place-blockchain-assurance/.

[10] Deloitte. « Blockchain applications in insurance », [En ligne]. https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdf.



ETHEREUM : DES APPLICATIONS DE PLUS EN PLUS NOMBREUSES

En plus du transfert d'actifs monétaires, d'obligations ou d'actions, la technologie *blockchain* peut également servir à la traçabilité des produits tout au long de la chaîne d'approvisionnement. La firme Provenance propose par exemple de suivre le parcours d'un thon depuis sa prise en Asie du Sud-Est jusqu'à sa vente dans une épicerie londonienne[11]. Une autre application similaire est également déjà proposée pour le marché diamantaire[12].

À titre de registre virtuel sécurisé, la *blockchain* peut aussi servir à prouver la propriété d'un bien ainsi que l'ensemble des transactions qui ont lieu autour de ce bien. Certains pays africains en voient l'application à titre cadastral et notarial, notamment pour résoudre les problèmes de corruption dans la gestion administrative[13].

Plusieurs grandes entreprises démontrent également de l'intérêt : « Microsoft offre à ses clients la possibilité d'exécuter des applications sur son architecture infonuagique nommée Azure et basée sur Ethereum. Deloitte a récemment établi un partenariat avec ConsenSys, une firme de développement sur Ethereum, pour concevoir une banque décentralisée et l'assureur Manuvie a mis en œuvre un projet en vue d'utiliser le réseau Ethereum au sein de sa division de gestion de patrimoine », conclut M. Hamel.

[11] Provenance. « Tracking tuna from catch to customer », [En ligne], 16 septembre 2016. https://www.provenance.org/news/technology/tracking-tuna-catch-customer/.
[12] http://www.everledger.io.
[13] Blockchain France. « Des cadastres sur la blockchain », [Blogue], 3 mars 2016. https://blockchainfrance.net/2016/03/03/des-cadastres-sur-la-blockchain/.

LEXIQUE

Bitcoin : cryptodevise décentralisée utilisée sur la *blockchain* originelle (voir aussi cryptomonnaie). Pour en savoir plus : bitcoin.fr.

Bloc : ensemble de transactions créées sur un réseau, validées et horodatées. Une fois ajouté à la chaîne, un bloc ne peut plus être modifié ni supprimé.

***Blockchain* :** technologie née pour servir de support à la cryptomonnaie Bitcoin. Par extension, tout réseau informatique basé sur cette technologie et fonctionnant comme un grand livre comptable virtuel dans lequel sont enregistrés les transactions et les soldes des utilisateurs et dont la mise à jour est effectuée par le réseau lui-même. Pour en savoir plus : blockchainfrance.net.

Contrats intelligents : programmes autonomes qui exécutent automatiquement les conditions d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.

Cryptomonnaie : monnaie électronique qui se base sur les principes de la cryptographie pour valider les transactions et la génération de la monnaie elle-même.

Ether : cryptodevise du réseau Ethereum. Voir aussi cryptomonnaie.

Ethereum : plateforme décentralisée basée sur la technologie *blockchain* qui permet de créer des contrats intelligents et qui fonctionne avec la monnaie ether. Pour en savoir plus : ethereum-france.com.

Mineur : individu ou entreprise qui connecte une ou plusieurs machines équipées pour effectuer du minage sur le réseau. Chaque mineur est rémunéré au prorata de la puissance de calcul qu'il apporte au réseau.

Nœud : ordinateur relié au réseau et utilisant un programme qui relaie les transactions.

Oracle : service ou individu responsable d'entrer manuellement une donnée extérieure dans la *blockchain* afin de valider l'exécution d'un contrat intelligent. Pour en savoir plus, consultez l'article « Les Oracles, lien entre la blockchain et le monde » sur ethereum-france.com.

***Smart contracts* :** voir contrats intelligents.