# 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.*

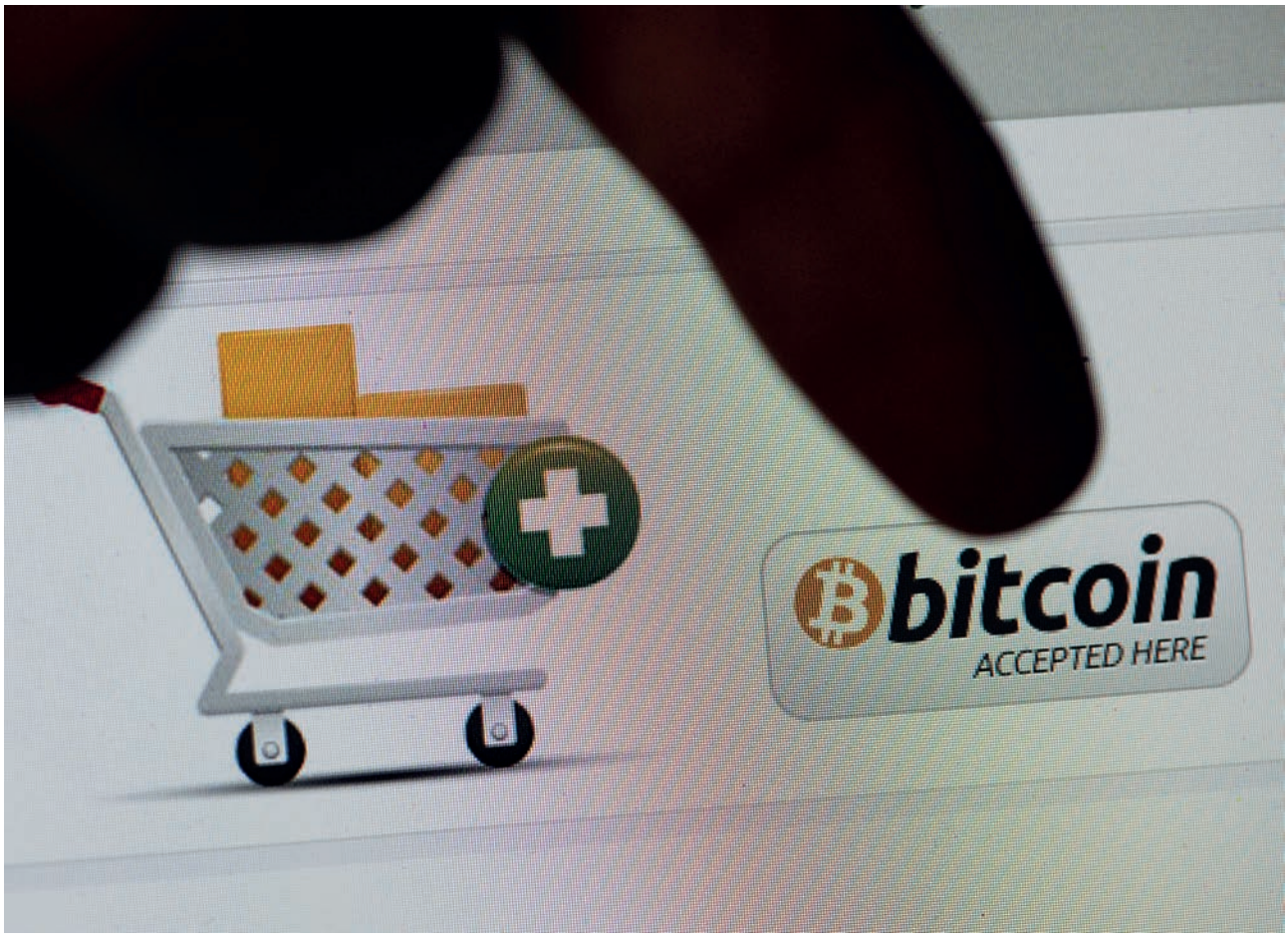


Photo © Jens Kalaene/Picture alliance-ZB-MAXPPP

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 ».

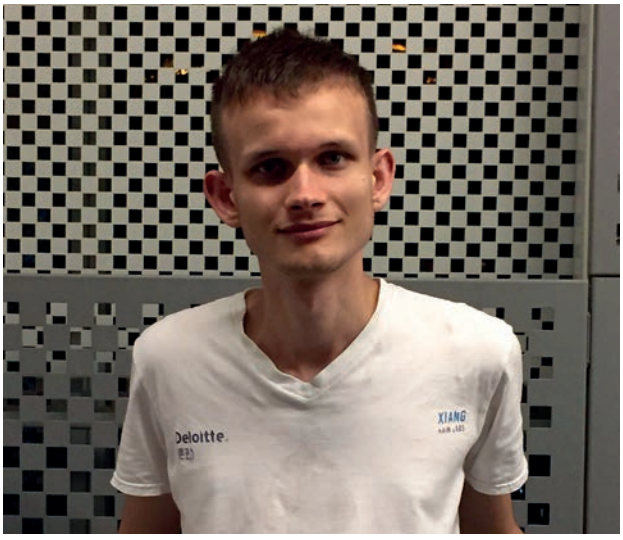


Photo © Romanpoet Wikimedia

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.