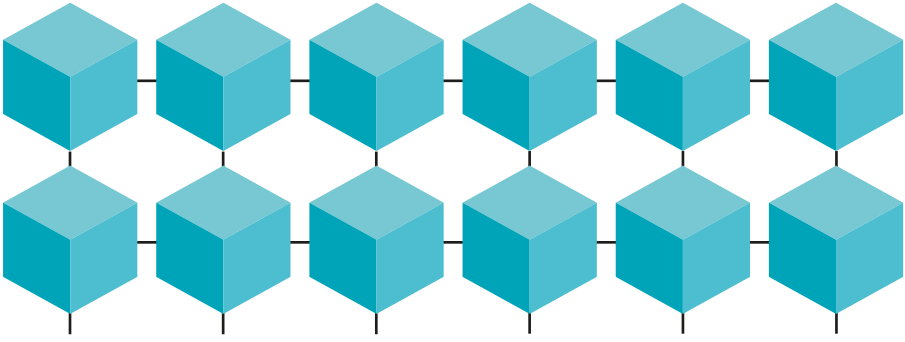
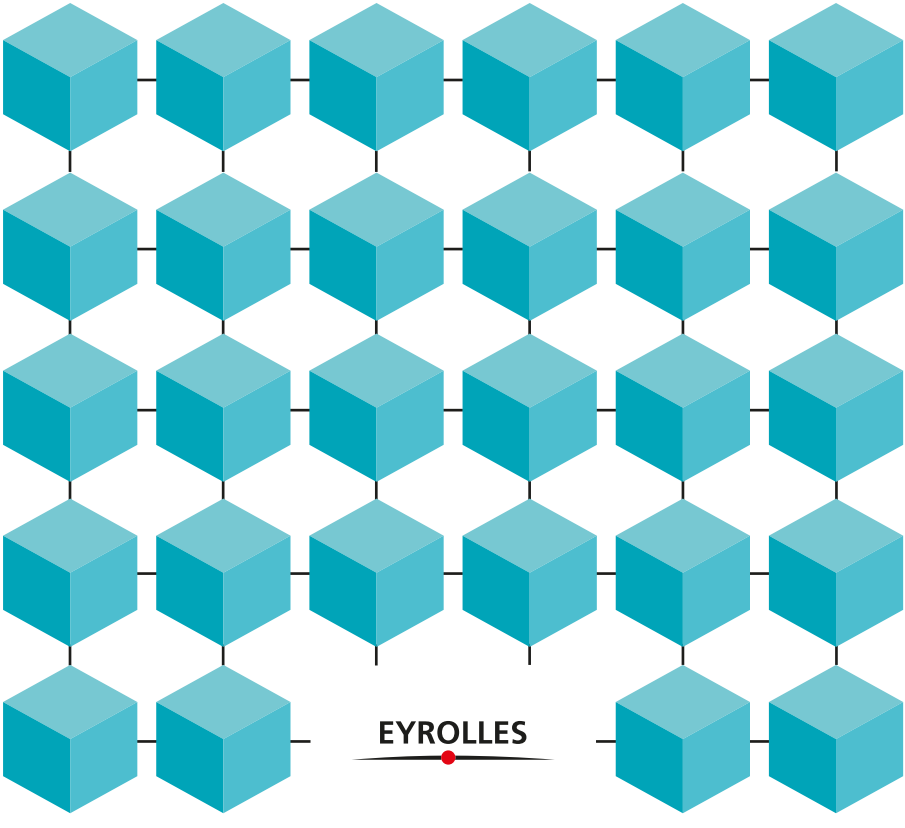


LAURENT LELOUP
Préface de William Mougayar

BLOCKCHAIN

La révolution de la confiance



EYROLLES

LA TECHNOLOGIE QUI POURRAIT « UBÉRISER UBER »

« Deuxième révolution numérique », « ubérisation ultime », « machine à confiance »... la blockchain laisse présager une révolution des usages comparable à celle portée par l'Internet dans les années 90.

La promesse de la blockchain est en effet majeure : des transactions instantanées à des coûts minimes et sans organe central de contrôle. Cette technologie a le potentiel de totalement changer les règles du jeu dans de nombreux secteurs économiques, à commencer par le système bancaire.

Comment se préparer ? Laurent Leloup décrypte de façon très pédagogique le fonctionnement d'une blockchain, les expériences en cours, les perspectives. Surtout, il pointe les questions à se poser et aide à diagnostiquer les opportunités liées à la blockchain dans chaque secteur.

Au-delà des implications économiques, c'est une profonde transformation sociétale qui s'annonce. Car la blockchain est avant tout une révolution de la confiance, portée non plus par un tiers de confiance – banquier, notaire, etc. –, mais par un système décentralisé et partagé. Un nouveau monde se profile.

Laurent Leloup *a fondé en 2006 Finyear Group, qui publie les quotidiens* Finyear & Blockchain Daily News *et produit de nombreux événements. En 2016, il a cofondé Blockness, une startup centrée blockchain, France Blocktech, l'association de l'écosystème blockchain français, et Blockchain Valley (campus, centre de formation, incubateur).*

www.editions-eyrolles.com

Blockchain

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Illustrations : Pierre Leloup

ISBN : 978-2-212-56665-9

Laurent Leloup

Blockchain

La révolution de la confiance

EYROLLES

Sommaire

Chapitre 3
La blockchain en pratique

Chapitre 4
La blockchain demain

À mon épouse Marie,

et à mes fils Yohan et Pierre

Préface

La blockchain est le meilleur nouvel outil de cette décennie. Pourtant, en ce début 2017, ce sujet connaît toujours un grave déficit de compréhension et de sensibilisation de la part du grand public. C'est un point de départ problématique pour la pleine réussite de son évolution.

Voici pourquoi le travail de Laurent Leloup dans ce livre est si important, car il nous aide à comprendre la blockchain, ainsi que ses multiples caractéristiques.

Bien que ce livre vous soit d'une grande aide pour comprendre la blockchain, cela n'est pas suffisant, car vous devez également vous entraîner à « comment penser blockchain ». Votre devoir, pour vraiment vous lancer dans un projet blockchain, sera de faire preuve de curiosité sur le sujet car tout n'est pas évident à comprendre de prime abord.

Dire que la blockchain est polyvalente est un euphémisme. Selon qui vous êtes et ce que vous faites, la blockchain aura quelque chose de différent à vous offrir. Ainsi, pour un développeur, la blockchain sera l'environnement de développement le plus excitant depuis l'avènement du langage Java en 1995, tandis que, pour une entreprise, la blockchain sera un puissant catalyseur pour la réingénierie des opérations commerciales et des relations externes, alors que pour un entrepreneur, la blockchain permettra de disrupter et d'inventer de nouveaux modèles sans crainte de se lancer avec simplement un petit nombre de clients.

La blockchain n'est pas un seul et même objet, un produit unique, une simple tendance ou une fonctionnalité particulière. La blockchain est composée de multiples pièces dont

certaines d'entre elles travaillent ensemble, et d'autres d'une façon autonome et indépendante. En raison de ces caractéristiques modulaires, la blockchain offre un éventail infini de choix d'applications.

L'évolution de la blockchain véhicule beaucoup d'ambition. Bien que la théorie de la blockchain soit bien systématique, comme vous le découvrirez dans ce livre, plus vous pourrez combler les écarts entre la théorie et la pratique avec des cas réels (*a priori* les vôtres ?) et plus vous diminuerez le nombre d'obstacles sur le chemin qui vous conduit vers la réussite du déploiement de vos propres cas d'usage.

Le message de la blockchain est simple, mais fort : il s'agit avant tout d'innover. Il ne s'agit pas seulement de découvrir un meilleur Web, d'inventer une meilleure banque ou de fournir un meilleur service. La survie de la blockchain dépendra de ce que vous en ferez, et cela ne reposera pas seulement sur ses caractéristiques techniques. Son adoption sera progressive, à commencer par les développeurs et les start-upers, puis par les gens du techno-business, suivis par les entreprises qui découvriront le potentiel du changement, puis du grand public qui exigera les changements, et enfin des organisations qui avaient jusqu'alors résisté au changement.

Mais pour y arriver, nous aurons besoin de plus d'utilisateurs d'applications blockchain, de plus d'applications à créer, et de beaucoup plus de développeurs. À long terme, la plupart des utilisateurs ne sauront pas ou ne réaliseront pas qu'il y a une blockchain dans le logiciel ou le service avec lequel ils interagissent. Tout comme aujourd'hui, nous recherchons et évaluons les capacités d'une application en fonction de ses vertus, non pas parce qu'elle est une application mobile, ni parce qu'elle fonctionne sur une base de données, ni parce qu'elle est basée sur une technologie quelconque.

Au même titre que l'économie du Web, la blockchain créera une nouvelle économie, et nous ne devons pas perdre de vue ce potentiel. L'économie crypto-tech sera une économie fondée sur la confiance décentralisée (à la naissance), tant sur le plan politique que sur le plan architectural. La blockchain donnera un accès égal à tout le monde et réduira le niveau des obstacles à tous ses participants.

Alors que la diffusion et le partage de l'information étaient le créneau que le Web avait initialement abordé, la fonction de base de la blockchain est la transmission des valeurs. Voilà l'ampleur de la compréhension fondamentale que vous devez assimiler sur la blockchain – et presque tout ce qui suit émane de cette idée fondatrice.

En dépit de tout l'émoi qu'elle a engendré, nous devons garder à l'esprit que la blockchain est essentiellement une promesse de la technologie. Comme toute promesse, il faut du temps pour qu'elle se réalise. Mais pour remplir toutes ces promesses, nous aurons besoin de millions de développeurs compétents en technologie blockchain, de millions de business leaders, et de millions d'utilisateurs passionnés et engagés.

Tandis que l'avenir de la blockchain peut être vu à travers l'histoire du Web, ne regardons pas en arrière, hâtons-nous d'aller de l'avant.

Un grand merci à Laurent pour avoir repoussé les limites de notre compréhension de la blockchain, car la pédagogie est une tâche difficile mais aussi un noble défi à relever.

William Mougayar[1]

1. Auteur de *The Business Blockchain*, Wiley, 2016.

Introduction

Lorsque *The Economist* titrait en octobre 2015 : « Blockchain, the Trust Machine », le web et les réseaux sociaux ont très rapidement et massivement relayé l'article.

Pensez-donc, nous sommes fin 2015, le mot « blockchain » n'a pas encore atteint le pic de notoriété qu'il connaît aujourd'hui et le magazine *The Economist*, donc pas n'importe lequel, titrait en couverture que la blockchain était une machine à créer de la confiance et que la technologie derrière le bitcoin pourrait transformer la façon dont fonctionne l'économie, rien que ça.

En fait, de quoi réveiller n'importe quelle rédaction… Ce qui n'a pas traîné car, dans les heures puis les jours qui ont suivi, l'ensemble des blogs, quotidiens, magazines et autres médias relayaient « l'article choc », avec plus ou moins de vérités sur la techno blockchain, le bitcoin et autres crypto-machins. Mais bon, la dynamique était enclenchée et la bombe médiatique de *The Economist* avait fait son effet.

Depuis octobre 2015 la pression médiatique n'est quasiment pas retombée et le nombre d'articles produits par jour sur la techno blockchain, les monnaies numériques et autres *distributed ledgers* est tout simplement phénoménal…

Cette annonce aura eu au moins une vertu : celle de parler de la blockchain, du bitcoin, des crypto-monnaies et des protocoles de consensus distribués, et d'initier la formation du public à une technologie disruptive, qualifiée de « révolutionnaire » par Don Tapscott et en voie d'ubériser Uber, « l'ubérisation ultime », comme le déclarait Philippe Herlin lors d'une interview.

Un peu plus d'un an est passé et peu de projets ont vu le jour : beaucoup d'annonces mais peu de réalisations concrètes, hormis quelques prototypes en cours de développement. Mais, me direz-vous, n'est-ce pas le lot d'une technologie naissante ?

Par contre, ce qu'il faut retenir de tout cet emballement médiatique et des échanges multiples et variés qui s'en sont suivis, c'est que l'innovation de la blockchain, dixit Ludwig Siegele, l'auteur de l'article publié dans *The Economist*, ce n'est pas l'argent… mais la confiance.

Rendez-vous compte, une technologie révolutionnaire, qui va disrupter de nombreux modèles d'affaires, complètement transformer l'économie et la société, et qui apporte quoi comme innovation ? La confiance.

Nous voici maintenant au milieu du gué, la pression médiatique va baisser en régime, les consultants vont monter en compétence, les entreprises, grandes puis moyennes, vont s'approprier la technologie, les projets vont se multiplier, les cas d'usage également, la technologie va progresser, les investisseurs vont se réveiller et au bout du bout nous aurons une seule vision novatrice, celle de la confiance partagée. C'est cela la promesse de la blockchain.

Il ne faut pas chercher à comprendre si l'on va être disrupté, transformé, ubérisé, il faut chercher dans son propre *business model*, dans ses relations avec ses clients, ses fournisseurs, ses personnels, où et comment nous pouvons apporter de la confiance.

Après l'avènement d'Internet des années 1990 puis de la blockchain Bitcoin (et son bitcoin) de Satoshi Nakamoto, les générations X et Y nous ont récemment montré la voie de plus de partage et de transparence avec l'avènement des réseaux sociaux.

Le pari perdu d'Internet de placer l'humain au cœur de sa technologie pour plus de pouvoir et de liberté sera peut-être relevé par la technologie blockchain.

Aujourd'hui nous avons une technologie « trustnomics[1] » qui peut insuffler de la confiance dans l'économie, la démocratie, la société… Alors saisissons cette opportunité, relevons le défi et lançons les machines à créer de la confiance dans les organisations et entre les individus.
2017 sera l'année de la naissance de la confiance partagée.

1. http://www.trustnomics.net

Chapitre 1

La blockchain, c'est quoi ?

« Qui manque de connaissance
est sans cesse à la merci du changement. »
Rémi Belleau

Démystifier la blockchain

Définition

Définir la blockchain en quelques mots n'est pas chose aisée car selon son mode de pensée, ses acquis, ses expériences, chaque lecteur ne sera pas réceptif de la même façon à une définition ou à une autre.

Voici plusieurs définitions qui, *crescendo*, devraient vous permettre de mieux comprendre ce qu'est la blockchain :

- Simpliste : une blockchain est un grand livre de compte ouvert et accessible à tous en écriture et en lecture et qui est partagé sur un grand nombre d'ordinateurs à travers le monde.
- Basique : une blockchain est un logiciel qui stocke et transfère de la valeur ou des données *via* Internet, de façon transparente et sécurisée, et sans organe central de contrôle.
- Littérale : une blockchain désigne une chaîne de blocs (conteneurs numériques) dans lesquels sont stockées des informations de toute nature : transactions, contrats, titres de propriétés, œuvres d'art, etc.
- Généraliste : une blockchain est une technologie pour une nouvelle génération d'applications transactionnelles qui, grâce à un mécanisme de consensus collectif couplé avec l'utilisation d'un grand livre de compte public, décentralisé et partagé, établit la confiance, la responsabilité et la transparence tout en rationalisant les processus d'affaires.
- Technique : une blockchain est une nouvelle technologie de base de données s'appuyant et tirant pleinement profit d'Internet, du protocole libre, de la puissance de calcul et de la cryptographie. Cette base de données transactionnelle distribuée est comparable à un grand livre comptable

(registre ou *ledger*) dans lequel chaque nouvelle transaction est écrite à la suite des autres, sans avoir la possibilité de modifier ou d'effacer les précédentes. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds).

On peut aussi proposer cette définition, qui résume l'ensemble des précédentes : une blockchain est une base de données transactionnelle distribuée, comparable à un grand livre comptable décentralisé et partagé, qui stocke et transfère de la valeur ou des données *via* Internet, de façon transparente, sécurisée, et autonome car sans organe central de contrôle. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds). Chaque membre du réseau possède une copie à jour du grand livre (en temps quasi réel) et le contenu est toujours en phase avec l'ensemble des participants.

Ainsi, la blockchain :

- permet l'automatisation de la transaction en supprimant les tiers ;
- est un système de consensus distribué et de confiance partagée ;
- est une infrastructure de certification et de notarisation.

Les grands principes de la blockchain

Les principes sur lesquels est fondée la blockchain sont les suivants :

- le *grand livre distribué* ou *distributed ledger* ou registre 2.0 construit sur le modèle des livres comptables et partagé entre les participants ;

- la *décentralisation* et la *désintermédiation* : aucune autorité centrale ne contrôle la blockchain, il n'y a pas de tiers de confiance ;
- le *consensus* : le fait qu'une transaction soit acceptée ou rejetée est le fruit d'un consensus distribué et non d'une institution centralisée (différentes formes de consensus existent) ;
- l'*immutabilité* : il est impossible de modifier ou de supprimer des écritures ;
- la *confiance partagée* et la *transparence* : il y a partage des données, des opérations et du consensus.

En résumé, passer par un mécanisme de consensus collectif plus utiliser un grand livre ouvert, décentralisé et partagé entraîne la *confiance*, la *transparence* et le *partage*.

La blockchain ne se limite pas à la blockchain Bitcoin ou à la blockchain Ethereum[1]. En effet, ce n'est pas une blockchain, mais plusieurs types de blockchains qui existent, cohabitent, voire interagissent. Ainsi, une blockchain peut posséder des spécificités techniques pour des utilisations ou des applications particulières.

La technologie blockchain change les règles du jeu : moins de centralisation, moins d'autorité, plus de partage. Ainsi, la blockchain apporte une infrastructure de confiance algorithmique distribuée ou *consensus-as-a-service* (consensus à la demande).

C'est en abordant ces aspects « d'infrastructure » que de nombreux observateurs ont tenté de rapprocher la technologie blockchain avec Internet, voire ont considéré qu'elle dépasserait Internet.

1. Bitcoin et Ethereum : voir le chapitre suivant.