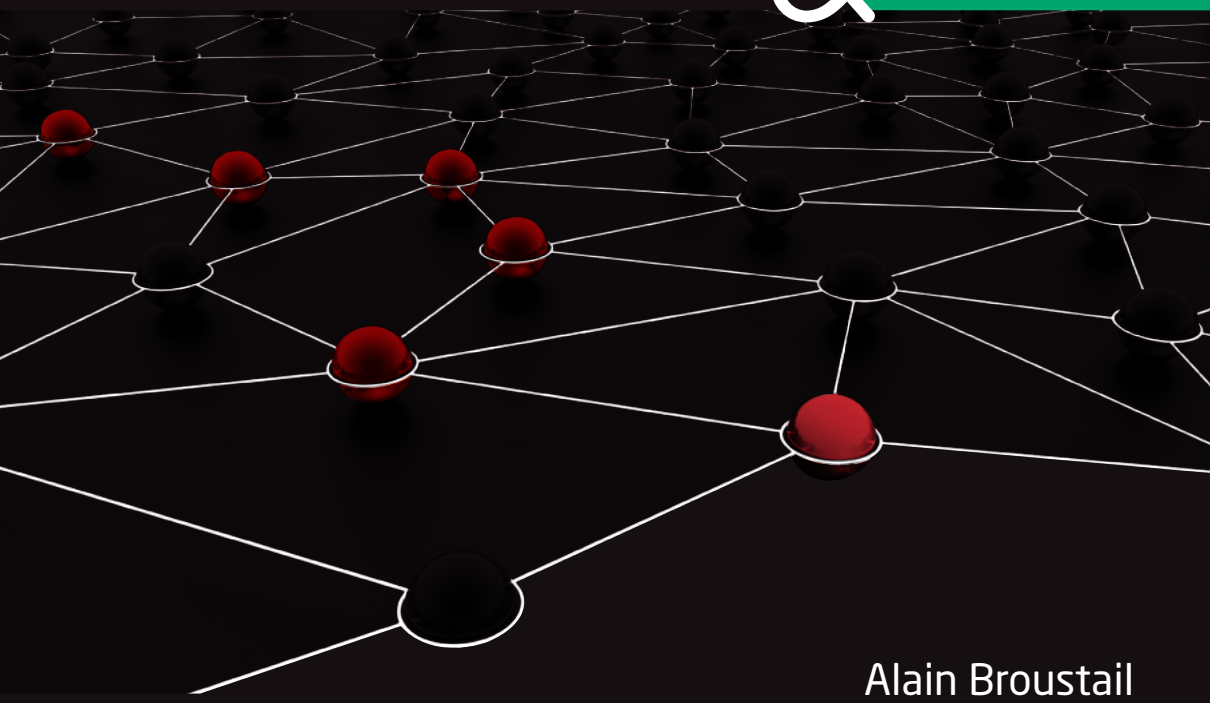
Information & stratégie



Alain Broustail

# Bien utiliser la technologie blockchain en entreprise

adbs

deboeck SUPÉRIEUR

# Bien utiliser la technologie blockchain en entreprise

Information & stratégie

regroupe des ouvrages pratiques et de réflexion destinés à l'entreprise et à ses professionnels, aux enseignants et aux étudiants concernés par la gestion de l'information et toutes les problématiques stratégiques qui y sont liées.

La collection s'adresse tant aux responsables marketing, communication, business analysts, RH, documentalistes, ingénieurs, chercheurs, bibliothécaires ou journalistes qu'aux étudiants et enseignants de ces filières. Elle fournit des outils et analyses de qualité, au contenu complet bien que concis, avec des exemples concrets et des illustrations. Des encadrés thématiques et une structure bien découpée permettent, au choix, une lecture fragmentée ou continue des ouvrages, toujours opérationnelle.

« Information & Stratégie » porte le label de l'**ADBS**, l'Association des professionnels de l'information et de la documentation, la plus importante association professionnelle de France dans le domaine des métiers de l'information. Créée en 1963, l'ADBS compte près de 3000 membres actifs.

La collection est dirigée par **Stéphane Cottin**, chargé de mission pour le développement des systèmes d'information et la valorisation des ressources documentaires auprès du cabinet du Secrétaire général du Gouvernement, et **Ghislaine Chartron**, professeur au Conservatoire national des arts et métiers de Paris (CNAM) et directrice d'un institut de formation des professionnels de l'information (INTD). Tous deux lui apportent leur expertise dans les domaines de l'information et de la documentation.

---

**DÉJÀ PARUS :**

*Alain Broustail*
*Bien utiliser la technologie blockchain en entreprise*

*Laurence Balicco, Evelyne Broudoux, Ghislaine Chartron, Viviane Clavier et Isabelle Pailliart (dir.)*
*L'éthique en contexte info-communicationnel numérique. Déontologie, régulation, algorithme, espace public*
*Actes du colloque « Document numérique et société », Échirolles, 2018*

*Joumana Boustany, Evelyne Broudoux, Ghislaine Chartron (dir.)*
*La médiation numérique : renouvellement et diversification des pratiques*
*Actes du colloque « Document numérique et société », Zagreb, 2013*

*Evelyne Broudoux, Ghislaine Chartron (dir.)*
*Big data – Open data. Quelles valeurs ? Quels enjeux ?*
*Actes du colloque « Document numérique et société », Rabat, 2015*

*Brigitte Simonnot, Evelyne Broudoux et Ghislaine Chartron (dir.)*
*Humains et données. Création, médiation, décision, narration*
*Actes du colloque « Document numérique et société », Nancy, 2020*

*Franck Bulinge*
*Maîtriser l'information stratégique. Méthodes et techniques d'analyse*

*Lisette Calderan, Pascale Laurent, Hélène Lowinger et Jacques Millet (coord.)*
*BIG DATA. Nouvelles partitions de l'information.*
*Actes du séminaire IST Inria, octobre 2014*

*Lisette Calderan, Pascale Laurent, Hélène Lowinger et Jacques Millet (coord.)*
*Publier, éditer, éditorialiser. Nouveaux enjeux de la production numérique*

*Gonzague Chastenet de Géry*
*Le knowledge management. Un levier de transformation à intégrer*

*Pascal Junghans*
*Les dirigeants face à l'information. Traitement, appropriation, décision*

*Véronique Mesguich, Armelle Thomas*
*Net Recherche 2013. Surveiller le web et trouver l'information utile*

*Véronique Mesguich*
*Rechercher l'information stratégique sur le web. Sourcing, veille et analyse à l'heure de la révolution numérique*

*Sébastien Rouquette (dir.)*
*Site internet : audit et stratégie*

*Jean-Michel Salaün, Benoît Habert (dir.)*
*Architecture de l'information. Méthodes, outils, enjeux*

*Frédéric Simonet*
*WordPress, Joomla, Drupal. Comprendre avant de s'engager : guide pratique des trois CMS les plus utilisés*

*André Tricot, Gilles Sahut, Julie Lemarié*
*Le document : communication et mémoire*

Information & stratégie

Alain Broustail

# Bien utiliser la technologie blockchain en entreprise

adbs

deboeck SUPÉRIEUR

Pour toute information sur notre fonds et les nouveautés dans votre domaine de spécialisation, consultez notre site web : **www.deboecksuperieur.com**

Couverture et maquette intérieure : cerise.be
Mise en page : PCA



Dépôt légal :
Bibliothèque nationale, Paris : juin 2021 ISSN 2295-3825
Bibliothèque royale de Belgique, Bruxelles : 2021/13647/078 ISBN 978-2-8073-3265-2

# SOMMAIRE

# CHAPITRE 1
# PRÉAMBULE

## 1.1 QUELQUES MOTS

Bienvenue dans le monde de la blockchain, un monde qui interroge, qui effraye, qui excite parfois, mais qui toujours soulève de la curiosité. Et comment ne pas en avoir lorsque l'on s'attarde un peu sur les crypto-monnaies et les sommes folles qui, parfois, s'échangent ?

Même les néophytes auront entendu parler de Bitcoin. Cette monnaie digitale a fait souvent parler d'elle lorsque, comme en 2017 ou fin 2020, elle a su créer des fortunes, et en défaire peut-être aussi, sur un principe et un fonctionnement que finalement peu d'investisseurs avaient alors compris. On l'a appelée *crypto-monnaie*, en référence aux technologies cryptographiques qui permettent son fonctionnement. Aujourd'hui, peut-être pourrions-nous la qualifier de *monnaie blockchain* pour être un peu plus précis sur son fondement technique. Et si Bitcoin fut la première et reste la plus importante d'entre elles, c'est loin d'être la seule sur le marché. Elle a inspiré la création de milliers d'autres, dont la variété d'objectifs et de fonctionnements ne serait comparable qu'avec la variété de tailles et de couleurs des poissons d'un récif corallien. Pour faire honneur au large éventail des cas d'usage adressés, il convient aujourd'hui de parler de crypto-actifs plus que de monnaie. Personnellement, nous sommes constamment émerveillé par la créativité folle que ces actifs numériques génèrent et nous essaierons de vous faire comprendre pourquoi nous restons ébahi devant l'excellence technique, l'insolence, le génie que leurs créateurs peuvent avoir.

Mais la blockchain, c'est aussi beaucoup plus que simplement les crypto-monnaies. C'est une technologie de gestion de données innovante et communautaire qui, utilisée à bon escient dans un contexte professionnel, présente d'énormes avantages par rapport aux approches informatiques plus traditionnelles.

D'une maturité toute relative, encore peu diffusée mais pourtant si prometteuse, la blockchain suscite de nombreux débats. Certains la trouvent révolutionnaire et associent même son aspect décentralisé et communautaire et transparent à un message politique, voire philosophique. De l'autre côté, ses détracteurs les plus ardents n'y voient qu'un gros et joli moelleux au chocolat qui un jour dégonflera, se refroidira et perdra tous ses attraits, telle une pyramide de Ponzi en fin de vie. Leur argumentaire est souvent très simple : « si c'était si utile, son utilisation serait déjà beaucoup plus courante ». Mais peut-être que sa relative rareté est encore due à une méconnaissance générale non seulement du grand public, mais aussi des professionnels en entreprise.

Ensemble, au long des pages qui vont suivre, nous allons découvrir son fonctionnement, ses caractéristiques et ce qu'il faut faire pour pouvoir en bénéficier.

Cet ouvrage fait avant tout office de vulgarisation. Si vous êtes novice sur le sujet, vous devriez pouvoir en ressortir avec de bonnes notions et une capacité à vous lancer dans vos premiers projets sur le sujet de manière sereine. Dans une optique pédagogique, certains points sur le fonctionnement des blockchains sont abordés plusieurs fois dans le livre. La répétition étant mère de l'apprentissage, nous avons préféré nous redire parfois plutôt que de prendre le risque de voir des notions clés mal comprises.

Si vous êtes déjà un expert, nous avons bon espoir que vous y apprendrez tout de même une chose ou deux et pourrez trouver matière à débat dans des positions sur certains sujets qui, parfois, seront très personnelles.

## 1.2 PRÉSENTATION DE L'OUVRAGE

En comptant ce préambule, ce livre est divisé en neuf chapitres qui peuvent se lire dans n'importe quel ordre. Nous vous recommandons cependant, surtout si vous découvrez le sujet, de les aborder dans l'ordre pour bénéficier à chaque fois de bases qui vous permettront de mieux comprendre la suite.

Tout d'abord, nous commençons par un **grand exercice de vulgarisation**. Si, pour vous, le discours des informaticiens ressemble trop souvent à du charabia, comprendre la blockchain reste possible ! Nous allons pour cela oser faire une comparaison un peu folle : en quoi la blockchain ressemble-t-elle à un fichier Excel ?

Sur ces bases partagées, nous vous embarquerons dans **l'histoire de la blockchain**, en partant des idées qui ont mené à la création de Bitcoin, la première blockchain, jusqu'à aujourd'hui.

Ensuite viendra **un état des lieux**, à fin 2020, sur le marché actuel de cette technologie, ses cas d'applications, ses acteurs les plus importants ; nous ferons également un peu de **prospective** sur ce qu'il pourrait devenir dans les prochaines années. Nous en profiterons aussi pour lister quelques projets d'entreprise du marché, prouvant la réalité actuelle de cette technologie.

Les esprits curieux auront envie d'en apprendre plus. Le chapitre suivant entrera dans de plus amples détails sur **le fonctionnement de la technologie**. Nous partirons systématiquement de l'exemple de Bitcoin, que nous étendrons souvent pour parler des autres blockchains (Bitcoin, après tout, a déjà 12 ans !). N'ayez crainte, même sans compétences informatiques particulières, vous devriez pouvoir tout comprendre ! Si vous aimez comprendre les choses, vous pouvez d'ailleurs lire ce chapitre avant les deux précédents, et bénéficier ainsi, peut-être, d'une meilleure maitrise du vocabulaire utilisé.

Lorsque vous lancerez votre projet, vous devrez choisir la technologie de registre distribuée qui vous convient. Et vous aurez le choix, comme vous pourrez le voir dans le chapitre « **Choisir sa blockchain** » que vous devriez pouvoir comprendre aisément, fort du bagage technique apporté par le chapitre précédent.

Sachant qu'aujourd'hui plus de 90 % du chiffre d'affaires réalisé grâce à la blockchain l'est sur des sujets de crypto-actifs, nous ferons ensuite un focus sur **les différents types d'actifs numériques**.

Arrivé à cette étape de l'ouvrage, si vous êtes un chef de projet expérimenté, vous pourriez arrêter votre lecture et entrainer votre entreprise dans de nouvelles aventures pleines de cryptographie, de « hash » et de « token » en tout genre. Nous vous invitons cependant à poursuivre encore un peu, pour bénéficier dans le chapitre 8 de quelques retours d'expériences et conseils à prendre en considération afin de **mener au mieux votre projet** et éviter certains écueils douloureux.

Nous irons plus loin, d'ailleurs, dans cette notion de conseil et conclurons avec un chapitre 9 dédié à l'étude de **trois exemples concrets** et des difficultés spécifiques que leur mise en œuvre pourra rencontrer.

# CHAPITRE 2
# COMPRENDRE L'ESSENTIEL

*Afin de pouvoir mieux comprendre les cas d'usage de la technologie blockchain, son histoire, son intérêt – sujets des chapitres à venir –, nous vous proposons de démarrer par la découverte du fonctionnement global de la technologie, en prenant souvent pour exemple la première d'entre elles – Bitcoin – qui nous servira tout au long de cet ouvrage d'étalon de comparaison avec les autres. Nous verrons avec quelle élégance son créateur, Satoshi Nakamoto, a assemblé plusieurs technologies déjà existantes pour construire quelque chose de particulièrement innovant.*

*Ce chapitre se veut accessible à tous et ne rentrera pas dans des détails techniques ; tout au plus devrez-vous être capable d'imaginer des fichiers Excel.*

*Au-delà des grandes caractéristiques d'une blockchain et de quelques éléments de vocabulaire, nous présenterons aussi rapidement le sujet des crypto-actifs, ainsi que les trois types de projets qui, à nos yeux, peuvent nécessiter l'utilisation de registre distribué.*

*Si vous maitrisez déjà de solides bases sur le fonctionnement d'une blockchain, n'hésitez pas à passer à la suite directement.*

## 2.1 VUE D'ENSEMBLE

Avant d'entrer dans les détails, il nous faut cependant prendre un peu de recul pour bénéficier d'une vue d'ensemble et examiner deux points importants pour une bonne compréhension du sujet.

### 2.1.1 Une blockchain, c'est avant tout du logiciel

C'est un programme informatique que l'on installe sur des ordinateurs en capacité de le faire fonctionner. Nous reprendrons l'analogie plus tard, mais il ne s'agit quelque part que d'un fichier Excel un peu sophistiqué. Et comme toute solution logicielle, elle peut évoluer dans le temps, donner lieu à de nouvelles versions, que cela soit pour corriger d'éventuels bugs ou pour apporter des améliorations à son fonctionnement. Le site Bitcoin.org liste ainsi une soixantaine de versions majeures de Bitcoin publiées depuis 2011.

https://bitcoin.org/en/version-history

Rien n'empêche non plus une équipe de développement de construire une nouvelle technologie blockchain, en partant de la page blanche,

ou en réutilisant certains composants logiciels préexistants « open source », des composants dont le code source a été rendu public par ses développeurs afin de permettre une vérification de son contenu par tout un chacun, souvent aussi pour en permettre une réutilisation facile par des tiers. Toutes les grandes blockchains en ont ainsi inspiré d'autres, qui parfois ont amélioré drastiquement le code source original, mais parfois aussi ne l'ont retouché que très subtilement, pour des différences qui, sans un œil expert, peuvent passer presque inaperçues.

Bitcoin a quelque part inspiré toutes les autres blockchains du marché. Certaines ne sont même que des copies presque conformes du code original de Bitcoin, des versions en quelque sorte parallèles de cette dernière, dont les plus connues s'appellent Bitcoin Cash, Bitcoin Gold ou Bitcoin SV.

### 2.1.2 Une blockchain, c'est aussi une communauté

Une blockchain n'a de sens que si elle est utilisée par une communauté de participants. Les objectifs et attentes qu'on peut en avoir – qu'on souhaite l'utiliser pour transférer des crypto-actifs, terme que l'on décrira en 2.3 et 7, ou pour partager des données – ne peuvent être atteints que par l'adhésion d'une multitude d'acteurs à l'utilisation de la même technologie.

Mettre en œuvre une blockchain pour un seul ou pour deux participants n'a aucun sens, on trouvera toujours de meilleures alternatives, d'autres solutions logicielles plus simples, plus efficaces à utiliser.

Plus le nombre de participants à un projet est important, plus l'utilisation d'un registre distribué (un autre terme pour parler de cette technologie) prend du sens. D'ailleurs, dans un contexte de blockchain publique, plus ses utilisateurs sont nombreux, plus ses qualités vantées – et en particulier sa sécurité – se concrétisent.

Au-delà de l'aspect informatique, le succès d'une blockchain dépendra de l'adhésion qu'elle suscitera. Il faudra donc accompagner son lancement d'une stratégie de communication pour faire connaitre et adhérer une communauté à son usage et à sa gouvernance.

Par gouvernance, nous entendons la définition de règles de fonctionnement et de collaboration entre membres du réseau. Comment par exemple s'assurer que tout le monde utilise bien la dernière version du logiciel ? Comment se mettre d'accord sur le contenu à inclure dans cette nouvelle version ? Qui va développer ces nouvelles fonctionnalités ? Comment limiter le risque d'abus d'usage, de fraude et de cyberattaque ? Quelle « économie » interne mettre en œuvre pour faire fonctionner toutes ces règles ?

C'est la combinaison de ces éléments qui fait de la blockchain une technologie si innovante. Et lorsque nous allons nous plonger dans son fonctionnement détaillé, il nous faudra toujours garder en tête qu'il s'agit d'une solution par et pour une communauté d'utilisateurs.

## 2.2 LA BLOCKCHAIN, UN FICHIER EXCEL DÉCENTRALISÉ ?

À des fins de vulgarisation pour nos lecteurs non informaticiens, nous allons dans ce chapitre comparer la blockchain avec un fichier Excel. Que les experts nous pardonnent pour les nombreuses simplifications faites.

### 2.2.1 Une base de données

Une blockchain, tout comme un fichier Excel, sert avant tout à stocker de l'information. Ce sont en quelque sorte des bases de données, bien qu'aujourd'hui ce terme soit plutôt associé à des technologies capables de stocker de l'information de manière massive et d'être requêtées de manière tout aussi massive (il en existe des centaines, telles que MS Access, SQL Server, Oracle DB, MongoDB, ou les bases de données cloud).

Ce n'est pas là le but d'une blockchain ou d'un fichier Excel, dans lesquels nous allons en général essayer de limiter la taille des données stockées au strict minimum, pour des raisons d'espace de stockage (les deux ont leurs limites), de performances (un fichier trop gros nécessite plus de ressources pour être manipulé) et, dans le cas de la blockchain, des coûts d'infrastructure associés.

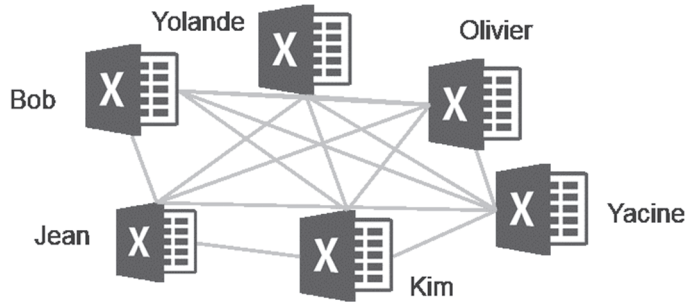
Le modèle de données d'un fichier Excel est en général très simple : des lignes et des colonnes dans un onglet unique. Le modèle de données de Bitcoin n'est pas beaucoup plus complexe.

C'est cette simplicité du modèle de données qui nous amène d'ailleurs à parler non pas de base de données, mais de **registre** de données (« ledger » en anglais).

À chaque cas d'usage son outil. La multiplication des bases de données en entreprise n'a pas empêché Excel de rester l'un des outils informatiques les plus populaires au monde. La blockchain n'a pas non plus pour ambition de concurrencer ni ces fichiers Excel, ni ces bases de données : son usage sera toujours restreint à des cas d'utilisation très précis.

### 2.2.2 Un fichier unique et décentralisé

Dans un stockage dit « en local », votre fichier Excel est stocké sur votre ordinateur. Dans sa version blockchain, il est non seulement installé sur votre poste, mais il est aussi répliqué sur l'ensemble des postes des membres de la communauté. Attention, il ne s'agit pas d'un fichier unique qui serait installé sur le cloud, et que tout le monde pourrait aller voir de manière simultanée – à l'image d'un fichier Excel qui serait stocké dans les applications Sharepoint online ou Teams d'une organisation. Ici, on parle véritablement de copies : chaque participant au réseau dispose d'une copie du fichier. Et comme ce fichier est voué à connaitre des modifications, la blockchain dispose d'un système de **synchronisation** permettant à tous les participants d'en avoir la même version.




Si Yolande, l'une des membres de cette communauté, se déconnecte de la blockchain par souhait ou par souci technique, les autres participants pourront quant à eux continuer d'y accéder et d'en utiliser les services. Et plus le nombre d'utilisateurs est important, moins l'absence de Yolande est préjudiciable. Lorsque cette dernière reviendra, son ordinateur se connectera au réseau, identifiera les membres encore présents et ira demander une mise à jour de son fichier Excel. Yolande recevra ainsi l'ensemble des données qu'il n'avait pas collectées pendant son absence.

Ce système est très résilient. Comparons maintenant cette approche avec celle proposée par un système de stockage dans le cloud. Reprenons votre fichier Excel, que l'on trouvera par exemple sur un espace MS Sharepoint Online, dans le cloud Azure. Si vous arrêtez de payer votre abonnement Office et que Microsoft supprime vos fichiers, vous aurez beau avoir eu jusqu'à 1 000 utilisateurs sur le fichier, ce dernier ne sera plus accessible à personne. Même chose si des hackers prennent le contrôle de l'administration de votre compte Office et vous en retirent les droits d'accès, ou si un gouvernement décide d'interdire l'utilisation des solutions Microsoft à sa population dans la nuit. Dans ces trois exemples, la centralisation de la gestion de l'information vous fait perdre l'accès à votre fichier. Dans le meilleur des cas, l'un des utilisateurs aura téléchargé localement (sur son poste) une version de sauvegarde mais, quoi qu'il arrive, vous n'aurez plus d'outil pour partager de manière simultanée des modifications aux fichiers.

La version blockchain de notre fichier Excel ne souffre pas de ce risque. Ici, les 1 000 utilisateurs à travers le monde en ont tous une copie en local. Quand bien même des hackers arriveraient à prendre le contrôle des postes de 100 membres de cette communauté, quand bien même un gouvernement interdirait l'usage d'Internet à 100 autres et une crise économique majeure couperait 100 utilisateurs d'électricité, il resterait encore 700 participants au réseau prêts à partager le fichier de données et à prouver son intégrité. Lorsque l'électricité reviendra, que l'attaque des hackers sera réglée, que ce gouvernement sans doute dictatorial sera tombé, les anciens participants à la blockchain pourront s'y connecter de nouveau et récupérer le fichier Excel dans sa dernière version. En attendant, ils en auront tous gardé une copie, dont les données étaient valables jusqu'à leur déconnexion.

Cet aspect décentralisé d'une blockchain publique fait partie des premiers gains visés par ceux qui en ont inventé le concept : son fonctionnement ne doit pas dépendre du bon vouloir d'une ou de plusieurs entités, fussent-elles des institutions publiques ou des groupes privés de très grosse taille.

On appelle donc généralement les technologies de blockchain **des technologies de registres distribués** (en anglais, Distributed Ledger Technologies, ou pour faire simple : DLT).

Les ordinateurs sur lesquels ces copies du fichier sont installées sont appelés des *nœuds* de la blockchain (ou « nodes » en anglais). Il peut exister différents types de nœuds, certains ayant par exemple une version complète des données, d'autres qui ne stockeront que les tout derniers messages.

### 2.2.3 Des données signées et horodatées

Notre communauté de blockchain publique est très ouverte : n'importe qui peut la rejoindre.

Et donc n'importe qui peut écrire dans notre fichier Excel. Certes, nous voulons éviter des abus d'usage, et nous allons donc mettre en place deux règles d'utilisation. La première c'est qu'écrire de l'information coûte un peu d'argent, ce qui évitera donc le risque de voir le système se faire « spammer ».

La seconde, c'est que toutes les transactions (échanges de données) sont signées. C'est-à-dire que lorsque l'on rajoute une ligne dans ce grand fichier Excel, on la signe et on horodate l'heure et la date de la saisie de l'information. Pour simplifier, imaginez que les trois premières colonnes du fichier Excel correspondent à un identifiant de transaction, à l'heure et la date de la saisie de la ligne, et à l'identité de la personne qui a inscrit cette ligne.

Attention cependant, lorsque l'on parle d'identité. Dans une blockchain, nous ne marquons jamais de nom ou de prénom. Nous travaillons dans un contexte de pseudo-anonymat : chaque utilisateur se voit attribuer une identité numérique (une longue chaine de caractères, générée au hasard, par exemple 0xea674fdde714Fd179de3edf0f56aa9716b898ec8). C'est à la responsabilité de chacun de décider s'il souhaite dévoiler ou non aux autres interlocuteurs son identité réelle. Techniquement parlant, nous verrons au chapitre 5 à quoi correspondent cette signature, cet horodatage et cette adresse.

À ce stade, il nous faut mentionner deux éléments importants :
- Il est possible de créer une blockchain « privée », dont les accès sont limités aux personnes que l'on souhaite inviter (comme un fichier Excel avec mot de passe). Nous en donnerons quelques exemples notamment en 6.3.
- Il n'est pas nécessaire dans les faits d'avoir une copie du fichier pour y inscrire une ligne. Il suffit de connaitre quelqu'un qui a le fichier et qui accepte de saisir des données en votre nom.

Fin 2019, on comptait ainsi environ 100 000 « nœuds » Bitcoin, pour plusieurs dizaines de millions d'utilisateurs uniques.

### 2.2.4 Des données qui se suivent, s'ajoutent, mais jamais ne s'effacent

Notre fichier Excel est un peu particulier. Il est en effet possible de rajouter des lignes, mais il n'est pas possible d'en effacer. Si Yolande souhaite rajouter une ligne (et qu'elle le fait dans le respect des règles imposées), c'est possible. Une nouvelle ligne sera ainsi insérée à la suite de la précédente, signée et horodatée.

Par contre, si elle souhaite supprimer une ligne déjà écrite, le système ne le lui permettra pas. Même s'il s'agit d'une ligne qu'elle a elle-même écrite. La règle est simple : on n'efface rien. Cela n'interdit cependant pas la création d'une nouvelle ligne qui se voudrait une fonction « Annule & Remplace ».

Dans l'esprit, on est très proche des règles d'une comptabilité exigeante, où aucune donnée passée n'est effacée, où l'heure et la date de saisie d'un élément sont importantes (ainsi que le nom de la personne l'ayant fait), et où les erreurs ne sont pas effacées, mais corrigées par des événements contraires. À la différence près que dans les faits un comptable motivé trouvera toujours un moyen de tricher dans sa comptabilité, alors qu'il est véritablement impossible de modifier les données inscrites dans une blockchain.

Cette immuabilité de l'information, dont on expliquera les causes techniques au chapitre 5, donne à toute blockchain un intérêt fort lorsqu'il existe un besoin de transparence et/ou de valeur probatoire autour des données inscrites.

### 2.2.5 Des données qui sont vérifiées avant de pouvoir être validées

Avant de voir sa nouvelle ligne inscrite dans le fichier Excel, plusieurs vérifications auront lieu :

- Toutes les inscriptions dans la blockchain étant signées, le système va en premier lieu vérifier que le message a bien été émis par le propriétaire légitime de la signature utilisée. On utilise pour se faire des technologies de cryptographie asymétrique, expliquée en 5.4.2.
- Il y aura des vérifications de format : tout comme dans un fichier Excel, on peut exiger de certaines données qu'elles répondent à un format spécifique : être une date, un chiffre, un texte de moins de vingt caractères, etc. Si une donnée envoyée ne correspond pas au format attendu, la transaction sera *a priori* rejetée dans son ensemble.
- La blockchain vérifiera la cohérence des données, et notamment vis-à-vis des données passées. Si par exemple nous procédons à une transaction de crypto-actifs entre deux parties, la blockchain vérifiera que l'émetteur dispose bien du montant qu'il souhaite envoyer.
- Des contrôles de cohérence métiers pourront aussi avoir lieu, au sein de ce que l'on appelle des « smart contracts » (on en parle

juste après). Si nous utilisons la blockchain pour des besoins de traçabilité logistique d'un poulet surgelé, nous aurons probablement instauré des règles pour vérifier si l'horodatage des transactions est possible : un poulet congelé le 04/08 peut-il avoir été mis en magasin le 02/08 ? Dans un fichier Excel, ce type de contrôle est parfois natif, il suffit de bien définir le type de données attendues dans une colonne (date/pourcentage/texte/…), mais peut aussi parfois nécessiter l'utilisation d'une macro. Il en va de même dans la blockchain, où les règles de vérification les plus complexes se feront à travers du code logiciel que nous appelons « smart contracts ».

Toutes ces vérifications sont faites automatiquement. Une fois réalisées, si aucune erreur n'est identifiée, notre grand fichier Excel se verra rajouter une ligne de plus, avec l'assurance que les données inscrites à l'intérieur répondent toutes au cahier des charges du fonctionnement du fichier. Dans les faits, pour des raisons de praticité, ces lignes ne sont pas vérifiées et écrites une par une, mais par blocs regroupant plusieurs centaines de lignes à la fois. Ces blocs se suivent les uns les autres, d'où le nom de « blockchain », chaine de blocs.

Notons que la réalisation de certains de ces contrôles nécessite de la puissance de calculs, de l'espace de stockage, et que seuls certains membres du réseau accepteront de mettre cette infrastructure à disposition pour procéder à ces vérifications. On les appelle dans Bitcoin les « mineurs ».

L'ensemble de cette procédure de collecte, vérification et diffusion des données porte le nom de « consensus ».

### 2.2.6 Un système capable d'évoluer vers des besoins complexes

Il est possible d'utiliser Excel pour inscrire sa liste de courses tout comme il est aussi possible d'y tenir l'intégralité de la comptabilité d'une société. L'utilisation combinée d'une multitude d'onglets, la maitrise de ses fonctions avancées, la création de macros complexes font encore en 2020 d'Excel un outil de gestion au centre de l'activité de nombreuses entreprises.

Cette évolutivité existe aussi pour les blockchains, en tout cas pour celles capables de gérer des smart contracts (plus de détails en 5.7). Comparables à l'utilisation de macros, acceptant des langages de programmation très complets, ces smart contracts permettent à un utilisateur avisé de créer son propre onglet de données dans une blockchain, avec ses propres règles : qui peut y accéder, ce qu'on peut y écrire, quelles sont les règles à respecter pour pouvoir y inscrire des données, création d'actions automatisées si certains critères sont respectés, etc.

Et gardons aussi en tête l'importante R&D (Recherche & Développement) qui a lieu dans le monde des technologies de registres distribués : de nouvelles solutions et des innovations arrivent sur le marché tous les mois, ce qui était impossible il y a encore peu

devient aujourd'hui réalité, demain la norme, et sera peut-être déjà obsolète peu de temps après.

### 2.2.7 Une gouvernance innovante

La plus grande invention de Bitcoin a peut-être été de prévoir dès le début un mécanisme incitatif pour garder dans la durée une communauté mobilisée et motivée à faire grossir la blockchain dans le respect de ses règles de fonctionnement.

Pour garantir ses éléments, l'inventeur de Bitcoin Satoshi Nakamoto a identifié le besoin que certains des participants du réseau mettent à disposition une infrastructure informatique pour stocker, vérifier et diffuser les données. Le monde n'étant pas fait que de bénévoles, Satoshi a défini des règles motivantes pour ces nœuds, que l'on appelle les mineurs. Prêter son infrastructure permet de gagner des bitcoins. Plus la blockchain est utilisée, plus ces bitcoins prennent de la valeur, et plus donc les mineurs ont intérêt à préserver le bon fonctionnement de cette communauté et par là même l'utilité des bitcoins qu'ils possèdent.

Chaque blockchain publique vient ainsi avec sa « crypto-économie », reposant sur l'utilisation d'un « coin », un actif numérique émis sur la blockchain. Les utilisateurs du registre distribué auront besoin de coins pour en payer les frais de transaction, et les mineurs qui mettent leur infrastructure au service du plus grand nombre sont rétribués dans la même devise digitale. Et ça fonctionne.

C'est l'utopie anarchiste à son maximum : un système autogéré, décentralisé (sans gouvernement ni police, sans éditeur de logiciel ni société derrière), fonctionnel, où chaque participant y trouve son intérêt *a priori*.

Bitcoin a ouvert la voie et de nombreux modèles de gouvernance et de crypto-économies alternatives ont par la suite vu le jour. Une blockchain publique ne peut fonctionner que si ces éléments sont clairs, cohérents et maitrisés.

Notons que si nous créons notre propre blockchain, pour un usage restreint à des membres invités, nous pouvons ensemble nous mettre d'accord sur des principes de fonctionnement différents. Si quatre entreprises décident de partager entre elles des données via une blockchain, elles arriveront probablement à mettre en œuvre une infrastructure et partager des frais de fonctionnement sans avoir besoin de créer une monnaie numérique qu'elles seraient seules à utiliser.

## 2.3 LES COINS, TOKENS ET AUTRES CRYPTO-ACTIFS

Le fonctionnement des crypto-actifs – terme générique que nous utiliserons pour l'ensemble de ces biens numériques échangeables sur blockchain – est extrêmement simple. Cependant, il est méconnu et entouré d'une aura qui souvent freine le grand public à sa compré-

hension. Les acteurs de la crypto-économie sont aussi en partie responsables de cette image. De nombreuses start-ups vont ainsi vanter l'innovation technologique majeure de leur token, unique dans son fonctionnement, plein de R&D, etc., alors qu'il n'en est souvent rien.

Tout d'abord, il faut préciser qu'il existe techniquement deux sortes de crypto-actifs, que l'on va appeler « coin » et « token ». Nous reverrons plus en longueur ces sujets au chapitre 7.

– Les « coins » : nous l'avons évoqué plus haut, une blockchain publique ne fonctionne que grâce à des principes d'incitation économique reposant sur le transfert d'une crypto-monnaie native à la blockchain. Chaque blockchain publique a ainsi impérativement besoin d'avoir son coin pour fonctionner (« coin » : à prononcer à l'anglaise, et non pas comme le cri du canard !).
– Les « tokens » : il s'agit des crypto-actifs que l'on crée en utilisant les fonctionnalités d'une blockchain déjà en place. Pour simplifier : je rajoute un onglet dans le fichier Excel décentralisé, et je décide de l'utiliser pour gérer des échanges de valeur. Pour ce faire, j'utiliserai un smart contract.

Rappelons ce que nous avons dit juste au-dessus : une blockchain, c'est un registre de données distribué et au modèle de données simple fonctionnant avec des règles propres et une infrastructure distribuée. Créer un token, c'est uniquement créer un nouveau registre de données au sein d'une blockchain déjà en place. Essayons de visualiser cela via un exemple simple.

Imaginons une société qui lance un nouveau token dont la possession permet de bénéficier de services divers. Cela pourrait par exemple être l'accès à des services de stockage de données – 1 token pouvant donner droit à 1 Go stocké pendant un an ; une monnaie virtuelle dans un jeu vidéo – 100 tokens permettant de s'acheter une maison dans le jeu, 1 000 tokens pour un château ; ou encore le droit à recevoir une partie des revenus d'une bourse en ligne – 1 token donnant droit à la distribution mensuelle de 0,00001 % des frais de transaction perçus par la plateforme sur la période.

Elle aura prévendu un certain nombre de ces tokens pour permettre de financer son projet (ce mode de financement porte un nom, c'est une « ICO : Initial Coin Offering »). Pour l'exemple, imaginons que ces tokens soient gérés sur la blockchain Ethereum, suivant l'exemple de l'immense majorité des ICO passées.

Techniquement parlant, notre start-up n'a fait que créer un nouvel « onglet » dans Ethereum, via la création d'un smart contract. Elle lui a associé un modèle de données simples, et quelques fonctions très basiques de transferts de token, probablement dans le respect d'une norme déjà prédéfinie et connue du marché (ex. : l'ERC20, la norme la plus utilisée sur Ethereum pour décrire le fonctionnement d'un crypto-actif simple).

Présentons-le dans un format Excel. En faisant abstraction de données techniques nécessaires pour la sécurité de la blockchain, voici à quoi ressembleront les données pertinentes du registre :

| Registre: les transactions | | | | |
|---|---|---|---|---|
| De qui | Vers qui | Pourquoi | Combien | Quand |
| START UP | - | Création initiale | 1 000 | 01/01/2020 |
| START UP | Yolande | Participation au financement du projet | 50 | 01/01/2020 |
| START UP | Yacine | Participation au financement du projet | 50 | 01/01/2020 |
| Yolande | Kim | Transfert | 10 | 02/01/2020 |
| Kim | Olivier | Transfert | 4 | 02/01/2020 |
| Yacine | Olivier | Transfert | 25 | 02/01/2020 |

| Registre : vue en stock | | | | |
|---|---|---|---|---|
| BLOCKCHAIN | YOLANDE | KIM | YACINE | OLIVIER |
| 1 000 | 0 | 0 | 0 | 0 |
| 950 | 50 | 0 | 0 | 0 |
| 900 | 50 | 0 | 50 | 0 |
| 900 | 40 | 10 | 50 | 0 |
| 900 | 40 | 6 | 50 | 4 |
| 900 | 40 | 6 | 25 | 29 |

Donnons quelques explications :

– Ligne 1 : Une start-up émet un token le 01/01/2020 (dans cet exemple, le smart contract est créé le jour même).
– Lignes 2 & 3 : Yolande et Yacine avaient donné de l'argent à cette start-up (via, par exemple, un virement bancaire sur le compte de la start-up) qui, en échange de ces fonds pour financer son projet, leur envoie maintenant à chacun 50 tokens comme prévu.
– Le 02/01/2020, Yolande transfère 10 tokens à Kim (ligne 4), Kim en retransfère immédiatement 4 à Olivier (ligne 5), qui en recevra aussi 25 de Yacine (ligne 6).

Rappelons que, dans les faits, la blockchain ne sait pas qui est Yolande ou Kim. Ces derniers sont représentés par des adresses de blockchain pseudo-anonymes, qu'ils auront préalablement envoyées à leur contrepartie pour recevoir les fonds (à l'image d'un identifiant IBAN bancaire).

Nous avons donc dans notre nouvel onglet créé un registre des transactions, et nous l'avons fait de manière à ce que tout membre de la blockchain disposant d'un nœud puisse vérifier l'exactitude des données et la réalisation concrète de l'échange.

Dans un système de paiement bancaire traditionnel, si vous souhaitez vérifier que l'argent de Kim a bien quitté son compte bancaire et est bien arrivé sur celui d'Olivier dans une autre banque, il va non seulement bien souvent falloir attendre un jour ou deux, mais en plus il faut comparer de chaque côté si les chiffres sont les mêmes. Une banque au système informatique défaillant pourrait ainsi en théorie oublier de créditer ou débiter un compte, ce qui est strictement impossible dans une blockchain où les transactions sont instantanées et vérifiables par tous.

Nous verrons au chapitre 7 qu'il existe de nombreux types de crypto-actifs. Nous avons pris plus haut l'exemple de tokens à valeur utilitaire, permettant à notre start-up de développer son

modèle économique. Imaginez maintenant que ces tokens représentent des actions d'une société. Nous avons avec la blockchain un registre de titre dématérialisé, infalsifiable, présentant de nombreux avantages par rapport au registre papier que toute société doit actuellement tenir elle-même (ou via ses avocats), et qui nécessite énormément de papiers et de signatures, surtout lorsque le nombre d'actionnaires est important. Il existe déjà des instruments financiers dématérialisés de cette manière sur blockchain, que l'on appelle des « security tokens ». Attention cependant, si leur fonctionnement technique est très similaire aux tokens à valeur utilitaire, leur nature juridique fait que l'émission et la vente de ces instruments financiers tokénisés sont soumises à une réglementation différente, plus contraignante.

Créer un token n'est pas forcément beaucoup plus compliqué que de créer un onglet dans un fichier Excel. La blockchain est un registre qui ne s'intéresse pas à la valeur du jeton, elle ne fait que les compter. Notre smart contract fonctionnera globalement de la même manière, que notre token représente littéralement de l'or en barre, des points de fidélité ou des jetons de poker virtuel. Il ne s'intéresse *a priori* ni au pourquoi du transfert (est-ce une vente ou un don ?), ni à la valeur possible de l'échange, ni au montant de l'éventuelle transaction financière qui a pu avoir lieu pour réaliser ces échanges. Il ne fait que lister les transactions digitales réalisées, principalement des échanges.

La valeur du token est ainsi fixée en dehors de la blockchain et correspond à ce que ses utilisateurs voudront lui fixer. Si la possession du token donne droit à un bien que l'on peut aller physiquement récupérer (par exemple un lingot d'or), il est aisé de comprendre que le token s'échangera à un prix proche de celui de son sous-jacent. Si le token donne droit à un service, comme des points de fidélité qui me permettraient d'accéder à des événements VIP, sa valeur sera *a priori* fixée de toute manière par l'offre et la demande. Car l'un des intérêts des crypto-actifs est qu'il est plutôt facile de mettre en place un marché d'échange, une bourse fonctionnant en temps réel et facilitant la mise en relation voire l'automatisation complète de la relation entre acheteurs et vendeurs.

Notons que si un token a une valeur financière, même faible, il est nécessaire de vérifier le contexte réglementaire dans lequel son échange est potentiellement encadré, ne serait-ce que pour des raisons comptables et fiscales (on évoque le point dans notre exemple du chapitre 9.2).

Si le token ne vaut financièrement rien, nous pourrons alors en faire ce que l'on en veut, au même titre que je peux rajouter ou effacer des colonnes dans Excel sans qu'aucune institution ne puisse *a priori* me demander des comptes.

## 2.4 LES CARACTÉRISTIQUES D'UNE BLOCKCHAIN, SON INTÉRÊT

### 2.4.1 Caractéristiques pertinentes

La technologie de blockchain publique présente les principales caractéristiques suivantes :

– la **décentralisation** : un réseau pair à pair où chaque nœud du réseau remplit une ou plusieurs fonctions ;
– la **transparence** : l'historique des transactions est consultable en permanence par n'importe qui via une connexion internet et un explorateur de blockchain, le code source d'une blockchain publique est ouvert et consultable par tous ;
– la **fiabilité :** la blockchain repose sur des mécanismes de cryptographie éprouvés et extrêmement robustes, tels que la gestion de binômes clés publiques/clés privées et des fonctions de hachage. De plus, les transactions sont toutes validées par des algorithmes (que l'on appelle consensus) avant d'être partagées au sein de blocs de données ;
– l'**immuabilité** : une fois insérée dans la blockchain, une transaction est infalsifiable, y compris par des acteurs malveillants qui participeraient au réseau ;
– l'**automatisation** : les transactions sont exécutées de manière autonome par des programmes informatiques sans recours à un tiers.

Le chapitre 5 sur le fonctionnement technique de la blockchain vous expliquera comment ces points sont atteints.

Certaines de ces caractéristiques peuvent se révéler particulièrement utiles lorsqu'elles sont appliquées au bon endroit.

### 2.4.2 Les trois types de projets auxquels s'adresse la technologie blockchain

Le paragraphe qui vient est plutôt subjectif et nous vient de notre expérience personnelle. Nous pensons en effet que la technologie de blockchain n'est appropriée qu'à trois types de besoins :

• l'**échange de crypto-actifs** ;
• la **création de preuves numériques** ;
• l'**échange collaboratif de données sensibles**.

#### 2.4.2.1 Échange de crypto-actifs

Si dans un projet j'ai besoin de pouvoir permettre à des particuliers ou des entreprises de s'échanger facilement des jetons numériques, qu'ils soient ou non associés à une valeur financière, la technologie blockchain est très pratique. Elle gère nativement la notion de compte, l'authentification de leurs propriétaires, elle permet les transferts et fait les comptes, elle vérifie la possibilité des échanges, le tout dans un contexte extrêmement sécurisé, et potentiellement totalement transparent (ou pas, au choix).

Nous reviendrons sur ces projets tant au chapitre 7 avec la classification d'actifs numériques qu'en 9.2 où nous regarderons ensemble

un exemple de projet (lancement d'un crypto-actif par un club sportif).

95 % du marché actuel de la blockchain tourne autour des crypto-actifs.

#### 2.4.2.2 La création de preuves numériques

**« La confiance n'exclut pas le contrôle ».**

Cette citation, attribuée à Lénine, est plutôt appropriée à ce que la blockchain permet de faire. Lorsque plusieurs individus ou entités cohabitent et collaborent, la confiance ne peut jamais être totale. Dans certains cas même, être paranoïaque est presque un prérequis si l'on veut réussir à faire des affaires dans de bonnes conditions.

Dans de nombreux cas d'usage métier, nous allons interagir avec d'autres entités, des personnes ou des sociétés, qui se sont engagées devant nous à respecter certains engagements. De manière réciproque, il nous sera demandé de prouver nos actes. Ce besoin de partage et de transparence peut autant avoir lieu en temps réel qu'*a posteriori*.

- **Temps réel** : Prenons l'exemple d'un bien acheté par e-commerce dont l'arrivée semble retardée. Je veux, maintenant tout de suite, savoir où il est, encore dans les mains du marchand ou déjà dans celles du coursier ? Qui dois-je appeler pour me plaindre ? Qui croire si les versions se contredisent ?
- ***A posteriori*** : Je n'ai jamais reçu mon achat. Je décide de porter plainte. Quelques semaines plus tard, au tribunal, le marchand appréciera disposer d'une preuve numérique prouvant qu'il avait effectivement remis en mains propres le bien au coursier en temps et en heure. Il prouvera ainsi le transfert de responsabilité de la perte du produit à ce dernier.

Ajoutons que, si le coursier avait été au courant de l'existence de cette preuve numérique, il aurait sans doute lui aussi accepté son tort plus facilement, ce qui lui aurait évité le passage au tribunal et aurait probablement arrangé tout le monde.

| #ID | De | Action | Quoi | Quand |
|---|---|---|---|---|
| 1 | Client ABL | Achat | Achat en ligne d'une TV Grand Ecran | 10/05/2019 à 14h |
| 2 | Marchand | Vente | Confirme la vente d'une TV Grand Ecran | 10/05/2019 à 17h |
| 3 | Marchand | Préparation | Confirme le démarrage de l'étape de préparation | 10/05/2019 à 17h30 |
| 4 | Marchand | Transfert | Confirme le transfert de la TV à "CoursierXYZ" | 11/05/2019 à 01h30 |
| 5 | CoursierXYZ | Réception | Confirme la réception de la TV à "CoursierXYZ" | 11/05/2019 à 01h30 |
| 6 | Client ABL | Plainte | Dépôt formulaire plainte - retard de livraison | 18/05/2019 à 03h15 |
| 7 | Marchand | Plainte | Confirme réception du dépôt de formulaire de plainte | 18/05/2019 à 03h15 |
| 8 | Marchand | Relance | Demande justificatif à CoursierRapide | 18/05/2019 à 03h16 |
| 9 | Marchand | Assurance | Déclare un possible litige à venir avec Client ABL et CoursierXYZ | 18/05/2019 à 03h16 |
| 10 | Assurance | Assurance | Confirme réception du message de Marchand | 18/05/2019 à 03h16 |

Exemple : si toutes les transactions avaient été tracées sur une blockchain, Client ABL n'aurait sans doute pas eu besoin d'aller au tribunal.

Parce que les données saisies dans la blockchain le sont en temps réel, parce qu'elles sont signées, parce qu'elles sont horodatées et surtout parce qu'elles ne peuvent pas être modifiées *a posteriori*,

Information & stratégie

En quelques années, les actifs numériques tels que le bitcoin sont passés de l'anonymat le plus total aux feux de l'actualité. Leur succès repose principalement sur la technologie sous-jacente à leur fonctionnement : la blockchain.

Appliquée aux problématiques d'une entreprise, la blockchain est un outil formidable pour stocker et partager de l'information de manière décentralisée, sécurisée et transparente. Récente, innovante, c'est une technologie qui est pourtant encore méconnue.

Accessible à tous, ce livre explique dans un langage non technique ce que sont les blockchains, leurs grands principes de fonctionnement, leurs marchés et leurs principaux cas d'usage.

Il se focalisera en particulier sur la mise en œuvre concrète de cette technologie dans un contexte professionnel. Le lecteur découvrira notamment les nombreuses spécificités d'un projet blockchain et sera capable, après sa lecture, d'évaluer par lui-même la pertinence et la faisabilité de ses idées au sein de son organisation.

Pour les **professionnels en entreprise** (cadres et dirigeants, techniciens et ingénieurs IT, marketing) ; pour les **professionnels de l'information et de la documentation** ; pour les **enseignants** et **étudiants** en information, communication, documentation et humanités numériques.

**ALAIN BROUSTAIL** partage dans cet ouvrage son expérience de consultant en innovation auprès des directions d'entreprises. Président de Blockchain EZ, un cabinet de conseil spécialisé dans les technologies de registres distribués, cofondateur de l'initiative open source Tezos DigiSign, il assure aussi la direction du pôle d'activité Blockchain de la société de services Sword France. Professeur vacataire au CNAM (INTD), il anime de nombreuses formations et conférences sur la blockchain et les crypto-actifs.

Créée en 1963, l'ADBS (Association des Professionnels de l'information) fédère une grande variété de professionnels de l'information numérique (veilleurs, knowledge managers, gestionnaires de contenus numériques, documentalistes, records managers, etc.). Elle compte près de 3000 membres en France. En 2013, l'ADBS s'associe aux éditions De Boeck pour créer la collection « Information & Stratégie » qui allie les savoir-faire des deux partenaires.

www.**deboecksuperieur**.com

ISBN 978-2-8073-3265-2
ISSN 2295-3825

9 782807 332652

Design cerise.be