

Avec les compliments d'IBM



La Blockchain

pour
les nuls[®]

Édition limitée IBM



Les fondamentaux
de la Blockchain

Faire de la Blockchain une
réalité pour l'entreprise

Démarrer un projet
Blockchain

Manav Gupta



La Blockchain

Édition limitée IBM

Manav Gupta

pour
les nuls[®]

La Blockchain pour les Nuls®, Édition limitée IBM

Publié par

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

Copyright © 2018 John Wiley & Sons, Inc.

Aucun extrait de cette publication ne peut être reproduit, stocké dans un système d'extraction de données ou transmis, sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement, numérisation ou autre), sauf aux conditions autorisées aux alinéas 107 ou 108 de la loi américaine sur le droit d'auteur (Copyright Act) de 1976, sans l'autorisation écrite préalable de l'Éditeur. Les demandes d'autorisation doivent être adressées par courrier à l'adresse : Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030 USA, par téléphone au +1 (201) 748-6011, par fax au +1 (201) 748-6008, ou en ligne à l'adresse <http://www.wiley.com/go/permissions>.

Marques : Wiley, la mention « pour les Nuls », le logo Dummies Man, The Dummies Way, Dummies.com, Making Everything Easier et les appellations commerciales s'y rapportant sont des marques ou des marques déposées de John Wiley & Sons, Inc. et/ou de ses sociétés affiliées aux États-Unis et/ou dans d'autres pays, et leur utilisation est interdite sans autorisation écrite. IBM et le logo IBM sont des marques déposées d'International Business Machines Corporation. Toutes les autres marques citées sont la propriété de leurs détenteurs respectifs. John Wiley & Sons, Inc., n'est lié à aucun des produits ou fournisseurs cités dans cet ouvrage.

LIMITATION DE RESPONSABILITÉ/EXCLUSION DE GARANTIE : L'ÉDITEUR ET L'AUTEUR S'ABSTIENNENT DE TOUTE DÉCLARATION OU GARANTIE CONCERNANT L'EXACTITUDE OU L'EXHAUSTIVITÉ DU CONTENU DE CET OUVRAGE, ET EXCLUENT EN PARTICULIER TOUTE GARANTIE, Y COMPRIS, NON LIMITATIVEMENT, LA GARANTIE D'ADÉQUATION AVEC UN USAGE PARTICULIER. AUCUNE GARANTIE NE PEUT ÊTRE CONSENTIE OU ÉTENDUE AU TITRE D'UN DOCUMENT COMMERCIAL OU PROMOTIONNEL. LES CONSEILS ET LES STRATÉGIES PRÉSENTÉS ICI RISQUENT DE NE PAS CONVENIR À TOUTES LES SITUATIONS. CET OUVRAGE EST COMMERCIALISÉ, SACHANT QUE L'ÉDITEUR NE DISPENSE AUCUN SERVICE JURIDIQUE, COMPTABLE OU PROFESSIONNEL. SI UNE ASSISTANCE PROFESSIONNELLE EST REQUISE, LES SERVICES D'UN PROFESSIONNEL COMPÉTENT DEVRONT ÊTRE SOLlicitÉS. NI L'ÉDITEUR, NI L'AUTEUR NE POURRONT ÊTRE TENUS RESPONSABLES DES DOMMAGES DÉCOULANT DES PRÉSENTES. LE FAIT QU'IL SOIT FAIT RÉFÉRENCE, DANS CET OUVRAGE, À UN ÉTABLISSEMENT OU À UN SITE WEB DANS UNE CITATION ET/OU À TITRE DE SOURCE POTENTIELLE D'INFORMATIONS COMPLÉMENTAIRES NE SIGNIFIE EN AUCUN CAS QUE L'AUTEUR OU L'ÉDITEUR APPROUVE LES INFORMATIONS SUSCEPTIBLES D'ÊTRE COMMUNIQUÉES PAR CET ÉTABLISSEMENT OU CE SITE WEB OU SES RECOMMANDATIONS. EN OUTRE, LE LECTEUR EST INFORMÉ QUE LES SITES WEB CITÉS DANS CET OUVRAGE PEUVENT AVOIR ÉVOLUÉ OU DISPARU ENTRE LE MOMENT OÙ CE LIVRE A ÉTÉ ÉCRIT ET CELUI OÙ IL EST LU.

Pour toute information d'ordre général sur nos autres produits et services, ou pour obtenir les informations nécessaires afin de créer un ouvrage *Pour les Nuls* destiné à votre entreprise ou à votre organisation, veuillez contacter notre service de développement commercial aux États-Unis par téléphone au 877-409-4177, envoyer un courrier électronique à l'adresse info@dummies.biz, ou visiter le site www.wiley.com/go/custompub. Pour de plus amples informations sur l'exploitation sous licence de la marque *Pour les Nuls* avec des produits ou services, contactez BrandedRights&Licenses@Wiley.com.

ISBN : 978-1-119-48446-2 (pbk) ; ISBN : 978-1-119-48450-9 (ebk)

Produit aux États-Unis

10 9 8 7 6 5 4 3 2 1

Remerciements

Parmi ceux qui ont participé à la création et à la commercialisation de cet ouvrage, figurent les personnes suivantes :

Éditrice de projet : Carrie A. Burchfield

Responsable éditorial : Rev Mengle

Éditeur, chargé des acquisitions : Steve Hayes

Représentante du développement commercial : Sue Blessing

Éditeur, chargé de la production : Vasanth Koilraj

Sommaire

INTRODUCTION	1
À propos de cet ouvrage.....	1
Hypothèses arbitraires	2
Les icônes utilisées dans ce livre.....	2
CHAPITRE 1 Les fondamentaux de la Blockchain	3
Blockchain : l'origine	3
Les inconvénients des systèmes de transactions existants	4
L'émergence du bitcoin.....	5
La naissance de la Blockchain	6
Révolution dans les réseaux d'entreprise traditionnels	6
Exploration d'une application Blockchain	7
Reconnaître les avantages clés de la démarche pour l'entreprise.....	9
Bâtir la confiance avec la Blockchain.....	11
CHAPITRE 2 Blockchain : comment ça marche ?	13
Que signifie « Blockchain » ?	13
Pourquoi la Blockchain est-elle appropriée pour les entreprises ?....	14
Registre partagé	15
Autorisations.....	15
Consensus	16
Contrats intelligents.....	17
Identification et rôles des participants	18
CHAPITRE 3 Dynamiser l'entreprise avec la Blockchain	19
Identifier les types de frictions commerciales.....	20
Frictions relatives aux informations	20
Frictions relatives aux interactions	20
Frictions relatives à l'innovation	21
Évoluer vers des réseaux d'entreprises sans friction.....	21
Réduire les frictions relatives aux informations.....	22
Atténuer les frictions relatives aux interactions.....	22
Atténuer les frictions relatives à l'innovation.....	23
Transformer les écosystèmes grâce à une visibilité plus large.....	24

CHAPITRE 4	La Blockchain en action : Cas d'utilisation	25
	Services financiers	25
	Financement professionnel	25
	Finance pour le commerce international	26
	Transactions internationales	26
	Assurance	27
	Administration publique.....	27
	Gestion de la chaîne logistique	28
	Santé.....	29
	Dossiers médicaux personnels	29
	Accords préalables de paiement	29
	Internet des objets (IoT).....	30
CHAPITRE 5	Hyperledger, projet de la Linux Foundation	31
	Les perspectives d'Hyperledger	32
	Hyperledger Fabric	33
	Que peut apporter IBM pour aider les développeurs à innover avec la Blockchain ?.....	34
	Un environnement cloud et une plate-forme de développement facilement accessibles.....	34
	Analyse individualisée et expertise sectorielle.....	35
CHAPITRE 6	Les 10 étapes clés de votre première application Blockchain.....	37
	Décider si la Blockchain a sa place dans votre secteur d'activité.....	37
	Identifier les freins aux processus métier	38
	Déterminer ce que peut vous apporter la Blockchain.....	38
	Choisir un cas d'utilisation approprié.....	39
	Déterminer la finalité de votre réseau Blockchain	39
	Identifier les dépendances.....	40
	Choisir un fournisseur et une plate-forme de Blockchain.....	40
	Développer et déployer le chaincode	41
	Tester et configurer votre application et votre réseau	41
	Participer à la plate-forme Hyperledger Rocket Chat Channel.....	41

Introduction

Bienvenue dans le livre *La Blockchain pour les Nuls*, édition limitée IBM, qui sera votre guide pour tout ce qui concerne la Blockchain pour l'entreprise. Selon certains, la Blockchain sera aux transactions ce qu'Internet a été pour l'information. C'est une approche qui permet d'apporter davantage de confiance et d'efficacité dans les échanges, quels qu'ils soient. La Blockchain peut transformer en profondeur la manière dont le monde travaille. Si vous avez déjà acheté un logement, vous avez probablement eu à signer quantité de documents papier, provenant de différents interlocuteurs, pour pouvoir mener à bien la transaction. De même, si vous avez déjà immatriculé un véhicule, vous imaginez sans peine les difficultés qui accompagnent cette démarche. Et je ne parle même pas de la complexité que représente le suivi de votre dossier médical personnel.

La technologie Blockchain, qui peut très simplement se définir comme un registre partagé et immuable, a tout le potentiel nécessaire pour transformer totalement l'ensemble des processus cités, et bien au-delà. Pour être très précis, aborder la Blockchain, ce n'est pas décrire le bitcoin. En revanche, je décris la fondation numérique sous-jacente qui permet de mettre en œuvre des applications *telles que* le bitcoin. Pour autant, la Blockchain va bien au-delà de ce type d'utilisation.

À propos de cet ouvrage

Le livre *La Blockchain pour les Nuls*, Édition limitée IBM, va vous permettre de découvrir la Blockchain, comment elle fonctionne et de quelle manière elle peut enrichir votre activité et le secteur dans lequel vous opérez. Vous y apprendrez les fondamentaux de la Blockchain et la façon dont cette technologie va révolutionner les transactions et les réseaux d'entreprise. Vous y découvrirez également la différence importante entre la Blockchain en général et son application à l'entreprise, et la raison pour laquelle il s'agit d'une solution idéale pour rationaliser les réseaux d'entreprise.

L'ouvrage aborde également Hyperledger, un projet de la Linux Foundation, conçu pour encourager l'évolution et la réflexion stratégique autour des technologies Blockchain issues de différents secteurs. Il y sera également question de l'environnement Hyperledger Fabric, plateforme open source, et du rôle essentiel qu'il joue dans le développement

de la Blockchain pour l'entreprise. Enfin, cet ouvrage vous apportera toutes les informations nécessaires pour déployer un réseau Blockchain.

Hypothèses arbitraires

J'ai rédigé ce livre à partir d'un certain nombre d'hypothèses au sujet du lecteur, c'est-à-dire vous. C'est ce qui m'a permis de définir son contenu et sa présentation pour les adapter au public approprié. En premier lieu, je vous ai imaginé tel un développeur relativement novice en matière de Blockchain, même si les parties moins techniques de cet ouvrage peuvent également intéresser les dirigeants d'entreprise et les décisionnaires. Quelle que soit votre fonction, je suis parti sur l'hypothèse d'élargir vos connaissances sur la Blockchain et son formidable potentiel. J'ai également supposé que vous souhaitiez en savoir davantage sur les différentes étapes à accomplir pour commencer à déployer des réseaux d'entreprise basés sur la Blockchain.

Les icônes utilisées dans ce livre

Les livres de la série *Pour les Nuls* comportent de petites images, baptisées icônes, placées en marge du texte. Ce livre utilise les icônes suivantes pour attirer votre attention :



ASTUCE

Cette icône indique les suggestions qui vous faciliteront la vie pour mettre en œuvre la Blockchain dans votre entreprise ou votre structure.



À RETENIR

Cette icône vous signale les concepts et les éléments importants à retenir.



ATTENTION

Cette fois, il ne s'agit plus de conseils. Les paragraphes signalés par cette icône attirent votre attention sur les pièges les plus courants.



SUR LE WEB

Cette icône permet de repérer où trouver, sur le Web, d'autres informations sur la Blockchain et les sujets qui s'y rapportent.

- » Exploration des racines du système de registre partagé
- » Découverte du potentiel de la Blockchain pour l'entreprise

Chapitre 1

Les fondamentaux de la Blockchain

La *Blockchain* est un registre partagé et distribué destiné à faciliter le processus d'enregistrement des transactions et de suivi des actifs dans un réseau d'entreprises. Un *actif* peut être un bien tangible (maison, voiture, liquidités, terrain), ou intangible, par exemple des éléments de propriété intellectuelle comme les brevets, les droits d'auteur ou les marques. Un réseau Blockchain permet de suivre et d'échanger pratiquement tout bien possédant une certaine valeur en réduisant les risques et en diminuant les coûts pour tous les interlocuteurs concernés.

Cette définition de la Blockchain est la plus succincte possible. La suite de ce chapitre abordera le sujet de manière plus détaillée pour vous permettre de mieux appréhender cette technologie et son potentiel de simplification des opérations métier.

Blockchain : l'origine

Pour mieux comprendre la démarche, il est nécessaire d'explorer le contexte dans lequel elle a été développée. À l'origine, les utilisateurs recherchaient un système efficace, rentable, fiable et sécurisé pour effectuer et enregistrer des transactions financières. Cette partie du livre va permettre de découvrir le contexte et les caractéristiques de la Blockchain qui en font une solution pour répondre de manière appropriée à cette attente.

Les inconvénients des systèmes de transactions existants

Tout au long de l'histoire, des instruments dignes de confiance, tels que les pièces de monnaie, les billets, les lettres de crédit et les systèmes bancaires, ont été développés pour faciliter l'échange de biens de valeur et protéger à la fois acheteurs et vendeurs. Grâce à des innovations importantes, en particulier le téléphone, les systèmes à cartes de crédit, l'Internet et les technologies mobiles, les transactions ont gagné en commodité, en vitesse et en efficacité, jusqu'à réduire, et même éliminer, toute distance entre acheteurs et vendeurs.



ATTENTION

Pour autant, nombre de transactions entre entreprises restent inefficaces, coûteuses et vulnérables, du fait des limitations suivantes :

- » Les liquidités ne sont utiles que pour les transactions locales et avec des montants relativement faibles.
- » Le délai séparant une transaction de son règlement peut être long.
- » La redondance des actions, la nécessité d'une validation par des tiers et/ou la présence d'intermédiaires contribuent à l'inefficacité de ce système.
- » La fraude, les cyberattaques ou même de simples erreurs contribuent aux coûts et à la complexité des activités. De plus, elles exposent tous les participants du réseau à des risques en cas d'atteinte d'un système central, comme celui d'une banque.
- » Les firmes spécialisées dans les cartes de crédit ont principalement créé des niches protégées, caractérisées par un prix d'entrée élevé. Les entreprises commerciales doivent payer des coûts d'entrée élevés pour leur inscription et leur intégration, ce qui implique des quantités considérables de documents papier et un processus de contrôle très fastidieux.
- » La moitié de la population mondiale ne dispose d'aucun accès à un compte bancaire et a été contrainte de développer des systèmes de paiement parallèles pour effectuer des transactions.

Les volumes de transactions à l'échelle mondiale progressent de manière exponentielle et vont à l'évidence amplifier la complexité, les vulnérabilités, l'inefficacité et les coûts des systèmes de transactions actuels. Le développement du commerce électronique, les activités de banque en ligne et les achats au moyen d'applications, ainsi que la mobilité croissante des utilisateurs dans le monde, ont contribué à l'augmentation des volumes de transactions. De plus, l'émergence de

l'Internet des objets (IoT) va accroître les volumes de transactions grâce à des objets autonomes, comme les réfrigérateurs qui achèteront des produits d'épicerie s'ils ne contiennent plus assez d'aliments, ou les voitures qui vous seront livrées à domicile, en passant, si nécessaire, à une station-service pour prendre du carburant.

Pour résoudre ces problématiques, entre autres, notre monde a besoin de réseaux de paiement rapides, disposant d'un mécanisme permettant d'établir la confiance, ne nécessitant aucun équipement spécialisé, sans frais ou redevance mensuelle, et assurant une tenue des comptes collective pour garantir confiance et transparence.

L'émergence du bitcoin

Le *bitcoin* est l'une des solutions développées pour répondre aux problèmes de complexité, de vulnérabilité, d'inefficacité et de coût des systèmes de transactions existants. Il s'agit d'une crypto-monnaie, lancée en 2009 par une ou plusieurs personnes dont l'identité reste mystérieuse, puisqu'elle n'est connue que par un pseudonyme : Satoshi Nakamoto.

Contrairement aux monnaies traditionnelles, émises par les banques centrales, le bitcoin ne dépend d'aucune autorité monétaire centrale. Personne ne le contrôle. Dépourvus de la forme matérielle des dollars ou des euros, les bitcoins sont « extraits » par des personnes (« mineurs »), et de plus en plus par des entreprises qui disposent d'ordinateurs partout dans le monde, avec des logiciels capables de résoudre des problèmes mathématiques. Plutôt que de s'appuyer sur une autorité monétaire centrale pour surveiller, vérifier et approuver les transactions et gérer la production de monnaie, les bitcoins sont traités par un réseau informatique de pair à pair, constitué par les machines de ses utilisateurs, comparable aux réseaux sur lesquels reposent BitTorrent et Skype.



ASTUCE

Le bitcoin a plusieurs avantages par rapport aux autres systèmes de transactions actuels, notamment :

- » **Rentabilité** : Le bitcoin élimine tous les intermédiaires.
- » **Efficacité** : Les informations relatives aux transactions sont enregistrées une seule fois et sont accessibles pour toutes les parties grâce au réseau distribué.
- » **Sûr et sécurisé** : Le registre associé possède des témoins d'intégrité. Aucune transaction ne peut être modifiée. La seule possibilité est de l'inverser, auquel cas l'une et l'autre restent visibles.

La naissance de la Blockchain

Le bitcoin est en réalité construit sur la base d'une Blockchain, qui sert de registre partagé pour cette monnaie. Vous pouvez considérer une Blockchain comme un système d'exploitation, tel que Microsoft Windows ou MacOS, le bitcoin n'étant que l'une des nombreuses applications pouvant fonctionner sur ce système d'exploitation. La Blockchain apporte un registre partagé permettant d'enregistrer les transactions en bitcoin. Mais ce registre partagé peut être utilisé pour consigner n'importe quelle transaction et suivre le mouvement d'un actif de nature tangible, intangible ou numérique. Par exemple, la Blockchain permet de régler les montants relatifs à des titres cotés en quelques minutes au lieu de plusieurs jours avec d'autres systèmes. Grâce au réseau Blockchain, les entreprises peuvent gérer leurs flux de marchandises et les paiements qui s'y réfèrent, et les fabricants peuvent partager leurs prévisions de production avec leurs sous-traitants (OEM) et les organismes réglementaires, afin de réduire les rappels de produits.



À RETENIR

Ce qu'il faut retenir : Bitcoin et Blockchain sont deux concepts *différents*. La Blockchain permet de stocker des transactions en bitcoins, mais elle a de nombreuses autres utilisations. Le bitcoin n'est en réalité qu'un premier exemple d'utilisation de la Blockchain.

Révolution dans les réseaux d'entreprise traditionnels

Avec les méthodes traditionnelles d'enregistrement des transactions et de suivi des actifs, les membres d'un réseau gèrent leurs propres registres, ainsi que d'autres documents, comme l'indique l'illustration sur la gauche de la Figure 1-1. Cette méthode traditionnelle peut s'avérer coûteuse, notamment parce qu'elle englobe des intermédiaires qui facturent des frais pour leurs prestations. L'approche est manifestement inefficace du fait des délais d'exécution des contrats et des actions redondantes nécessaires pour tenir plusieurs registres. Elle est également vulnérable car, si un système central (par exemple une banque) subit une atteinte du fait d'une fraude, d'une cyberattaque ou d'une simple erreur, l'impact touche l'ensemble du réseau d'entreprises.

L'illustration sur la droite de la Figure 1-1 représente des réseaux d'entreprises utilisant la Blockchain. L'architecture Blockchain apporte aux participants la capacité à partager un registre qui va être mis à jour, au moyen de répliquions de pair à pair, chaque fois qu'une transaction a lieu. La *réplication de pair à pair* signifie que chaque participant (nœud) du réseau agit à la fois comme un éditeur et comme un abonné.

Chaque nœud peut recevoir ou émettre des transactions vers d'autres nœuds, et les données sont synchronisées à l'échelle du réseau lorsque le transfert est effectué.

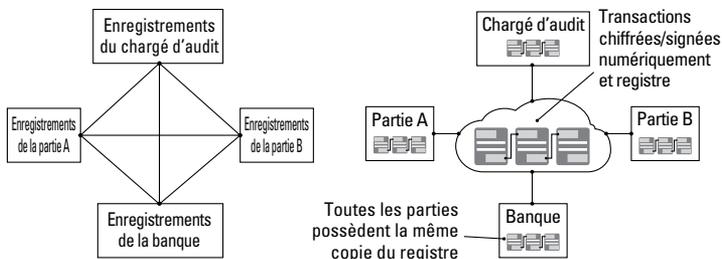


FIGURE 1-1 : Réseaux d'entreprises avant et après la Blockchain.

Le réseau Blockchain est économique et efficace, car il élimine la redondance des actions et réduit la nécessité des intermédiaires. Il est également moins vulnérable, puisqu'il utilise des modèles de consensus pour valider les informations. Les transactions sont ainsi sécurisées, authentifiées et vérifiables.



À RETENIR

Les participants des deux systèmes de transactions sont les mêmes. Le changement réside dans le fait que l'enregistrement de la transaction est partagé par toutes les parties et visible par tous.

Un réseau Blockchain possède les caractéristiques essentielles suivantes :

- » **Consensus** : Pour qu'une transaction soit valide, tous les participants doivent s'accorder sur sa validité. (Voir le chapitre 2 pour en savoir plus sur les mécanismes de consensus.)
- » **Provenance** : Les participants savent d'où provient l'actif et de quelle manière ses propriétaires ont changé au fil du temps.
- » **Immuabilité** : Aucun participant ne peut falsifier une transaction après qu'elle a été enregistrée dans le registre. Si une transaction provoque une erreur, il est nécessaire d'effectuer une nouvelle transaction pour l'inverser. Les deux transactions sont ensuite visibles.
- » **Finalité** : Un registre unique et partagé constitue un emplacement auquel chacun se réfère pour déterminer la propriété d'un actif ou la mise en œuvre d'une transaction.

Exploration d'une application Blockchain

Du point de vue des entreprises du secteur de l'automobile, la location d'un véhicule semble facile. En réalité, le processus est assez compliqué.

L'un des problèmes importants auxquels les réseaux de location de véhicules ont à faire face aujourd'hui est que, malgré l'intégration fréquente de la chaîne logistique physique, les systèmes pour la mettre en œuvre sont souvent fragmentés. Chacune des parties du réseau tient son propre registre, dont la synchronisation peut nécessiter des jours voire des semaines (voir Figure 1-2).

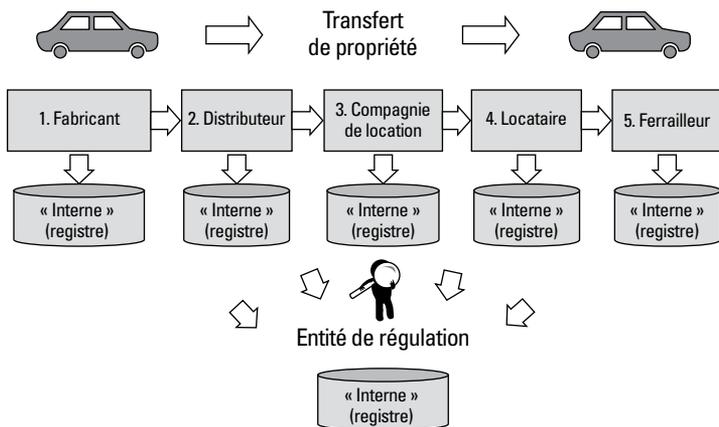


FIGURE 1-2 : Suivi des propriétaires successifs d'un véhicule en l'absence de Blockchain

En utilisant un registre partagé dans un réseau Blockchain, chaque participant peut connaître, surveiller et analyser la situation du véhicule, indépendamment de sa position dans le cycle de vie (voir Figure 1-3).

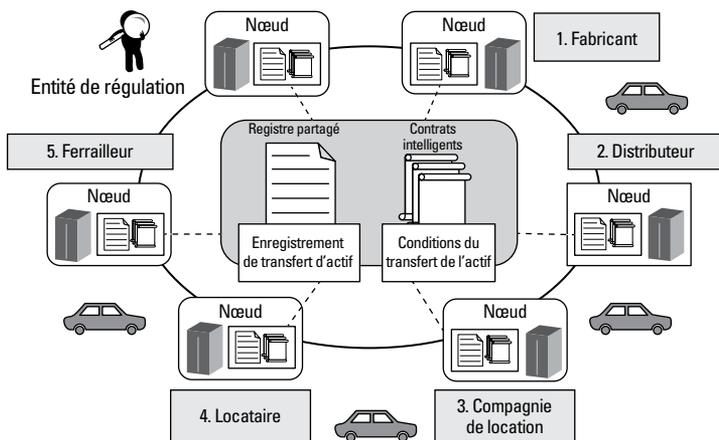


FIGURE 1-3 : Suivi des propriétaires successifs d'un véhicule avec une Blockchain

Avec la Blockchain, les membres du réseau peuvent interagir de la manière suivante :

1. **L'organisme régulateur gouvernemental crée et complète l'immatriculation du nouveau véhicule dans la Blockchain et en transfère la propriété au constructeur.**
2. **Le constructeur ajoute au formulaire le numéro de fabrication, de modèle et d'identification du véhicule dans les paramètres autorisés par le *contrat intelligent* (accord numérique ou ensemble de règles régissant une transaction — voir chapitre 2 pour en savoir plus).**
3. **Le concessionnaire peut visualiser la nouvelle disponibilité en stock et le véhicule peut être transféré du constructeur au concessionnaire après signature d'un contrat intelligent pour valider la vente.**
4. **La compagnie de location peut visualiser le stock du concessionnaire.**
La propriété du véhicule peut être transférée du concessionnaire à la compagnie de location après signature d'un contrat intelligent pour valider le transfert.
5. **Le locataire peut visualiser les véhicules disponibles à la location et compléter les formulaires requis pour signer le contrat de location.**
6. **Le processus de location se poursuit entre les différents locataires et la compagnie de location jusqu'à ce que celle-ci procède au retrait du véhicule.**

À ce stade, la propriété de l'actif est transférée au ferrailleur, qui, en vertu d'un autre contrat intelligent, est autorisé à éliminer le véhicule.

Reconnaître les avantages clés de la démarche pour l'entreprise

Pour une entreprise, la Blockchain offre les avantages spécifiques suivants :

- » **Gains de temps** : Les délais de mise en œuvre d'une transaction pour des interactions complexes impliquant de multiples parties sont ramenés à quelques minutes, contre plusieurs jours auparavant. Le règlement des transactions est plus rapide, car il ne nécessite aucune vérification par une autorité centrale.

» **Réduction des coûts** : Un réseau Blockchain permet de réduire les dépenses dans plusieurs domaines :

- La supervision est réduite, car le réseau est contrôlé de manière autonome par ses membres, tous connus les uns des autres.
- Les intermédiaires sont moins nombreux, car les membres du réseau peuvent échanger de manière directe des biens de valeur.
- La redondance des actions disparaît, car tous les membres du réseau ont accès au registre partagé.

» **Sécurité plus robuste** : Les fonctionnalités de sécurité de la Blockchain protègent le réseau contre les falsifications, la fraude et la cybercriminalité. S'il s'agit d'une Blockchain privée (*permissioned*), elle permet la création d'un réseau réservé aux membres, assorti de preuves garantissant leur identité et la nature exacte des biens ou des actifs échangés tels qu'ils sont représentés.



ASTUCE

Tous les réseaux Blockchain ne sont pas adaptés à l'entreprise. Certains sont privés, mais pas tous. Un réseau privé, qui impose des autorisations, est critique pour une Blockchain d'entreprise, en particulier pour les secteurs réglementés. Ce type de réseau offre les avantages suivants :

» **Confidentialité accrue** : Grâce à l'utilisation d'identifiants et d'autorisations, les utilisateurs peuvent définir les détails des transactions que les autres membres peuvent visualiser. Il est possible d'étendre les autorisations à des utilisateurs spéciaux, par exemple les chargés d'audit, qui peuvent avoir besoin d'accéder à d'autres détails relatifs aux transactions.

» **Facilitation des audits** : L'existence d'un registre partagé constituant une source de fiabilité unique accroît les possibilités de surveiller et de vérifier les transactions.

» **Plus grande efficacité opérationnelle** : Le traitement purement numérique des actifs permet de simplifier le transfert de propriété et les transactions peuvent être effectuées à une vitesse plus proche du rythme des activités.

Le chapitre 2 aborde de manière plus détaillée les caractéristiques qui font du réseau Blockchain une solution idéale pour l'entreprise.

Bâtir la confiance avec la Blockchain

Une Blockchain contribue à accroître la confiance au sein d'un réseau d'entreprises. Pouvez-vous faire confiance ou non à ceux qui font des affaires avec vous ? Dans un réseau Blockchain, vous n'avez pas à vous en soucier.

Une Blockchain est particulièrement intéressante pour accroître le niveau de confiance entre les membres d'un réseau. Toutes les transactions étant fondées sur d'autres transactions, la moindre corruption est immédiatement apparente, et chaque membre en est informé. Cette régulation autonome permet de limiter la dépendance vis-à-vis du niveau des protections et des sanctions légales et gouvernementales en vigueur pour surveiller et contrôler le flux de transactions métier. C'est le rôle de la communauté des membres.

Lorsqu'un contrôle par un tiers est requis, la Blockchain réduit la charge incombant au système de régulation en facilitant l'examen des détails des transactions et la vérification de la conformité par les chargés d'audit et les intervenants régulateurs.

Une Blockchain suscite la confiance grâce à cinq caractéristiques principales :

- » **Distribuée et pérenne** : Le registre est partagé, mis à jour à chaque transaction et dupliqué sélectivement par les membres, quasiment en temps réel. Puisqu'elle n'est soumise ni à l'appartenance, ni au contrôle d'une structure unique, l'existence durable d'une plate-forme Blockchain ne dépend pas d'une entité individuelle.
- » **Sécurisée, privée et indélébile** : Les autorisations et la cryptographie évitent tout accès non autorisé au réseau et garantissent que les membres sont bien ceux qu'ils prétendent être. La confidentialité est assurée grâce à des techniques cryptographiques et/ou de partitionnement des données grâce auxquelles les membres bénéficient d'une visibilité sélective sur le registre ; il est possible de masquer à la fois les transactions et l'identité des parties qui les ont effectuées. Lorsque des conditions ont été convenues, les membres sont dans l'impossibilité d'altérer un enregistrement de transaction et les erreurs ne peuvent être résolues que par de nouvelles transactions.
- » **Transparente et contrôlable** : Les participants engagés dans une transaction ont accès aux mêmes dossiers. Ils peuvent donc valider les transactions et vérifier les identités ou la propriété

sans nécessiter d'intermédiaires tiers. Les transactions sont horodatées et vérifiables en temps quasi réel.

- » **Basée sur un consensus et transactionnelle** : Tous les membres du réseau concerné doivent s'accorder sur la validité d'une transaction. Ce processus s'appuie sur des algorithmes de consensus. Chaque réseau Blockchain établit les conditions dans lesquelles une transaction ou un échange d'actifs peut avoir lieu.
- » **Orchestrée et flexible** : Les règles métier et les contrats intelligents (dont la mise en œuvre repose sur une ou plusieurs conditions) pouvant être placés sur la plateforme, les réseaux Blockchain peuvent évoluer au fil de leur maturité pour intégrer les processus métier de bout en bout et un très large éventail d'activités.

- » Analyse du concept de « Blockchain »
- » Pourquoi la Blockchain est-elle appropriée pour les entreprises ?
- » Identification et rôles des membres du réseau

Chapitre 2

Blockchain : comment ça marche ?

Le chapitre 1 vous a apporté des connaissances générales sur ce qu'est la Blockchain et ce qu'elle peut vous permettre de faire. Mais peut-être vous demandez-vous comment elle fonctionne. Dans ce chapitre, j'aborde le sujet en vous faisant visiter les coulisses d'un réseau Blockchain, sans toutefois être excessivement technique.

Vous y apprendrez comment un réseau Blockchain stocke les transactions pour éviter que celles qui sont enregistrées ne soient modifiées. Vous y découvrirez également les quatre concepts fondamentaux d'un réseau Blockchain pour l'entreprise, vous y rencontrerez les membres du réseau et vous pourrez vous faire une idée des différents rôles qu'ils jouent.

Que signifie « Blockchain » ?

Le terme *Blockchain* provient de la manière dont le réseau stocke les données relatives aux transactions, c'est-à-dire des *blocs* (block en anglais), reliés pour former une *chaîne* (chain en anglais) (voir Figure 2-1). La « chaîne de blocs » s'étend ainsi au fur et à mesure de l'augmentation du nombre de transactions. Les blocs recueillent et confirment les heures et les séquences des transactions, ainsi consignées dans la Blockchain, dans un réseau distinct, régi par des règles convenues entre ses membres.

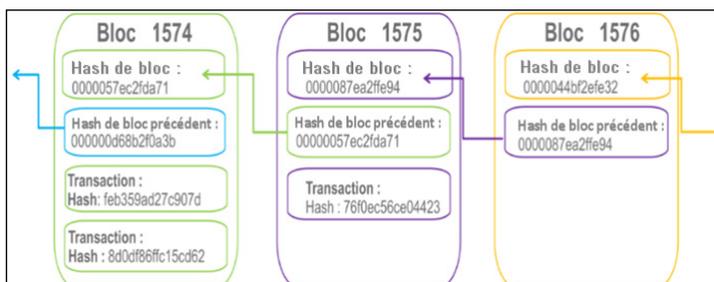


FIGURE 2-1 : La Blockchain stocke les enregistrements de transactions sous la forme d'une série de blocs reliés.

Chaque bloc contient un *hash* (empreinte numérique ou identifiant unique), les lots horodatés des transactions récentes valides et le hash du bloc précédent. Le hash du bloc précédent relie les blocs ensemble et évite qu'un bloc ne soit modifié ou inséré entre deux blocs existants. Ainsi, chaque bloc consécutif renforce la vérification du précédent, et, par conséquent, l'ensemble de la Blockchain. La Blockchain contient donc des témoins d'intégrité qui lui confèrent sa caractéristique essentielle d'immuabilité.



À RETENIR

Pour être très précis, même si la Blockchain contient des données de transaction, elle ne vient *en aucun cas* remplacer les bases de données, les technologies de messagerie, les traitements transactionnels ou les processus métier. Elle contient tout simplement des preuves de transactions vérifiées. Pour autant, même si une Blockchain sert pour l'essentiel de base de données d'enregistrement de transactions, ses avantages vont bien au-delà de ceux d'une base de données traditionnelle.

Pourquoi la Blockchain est-elle appropriée pour les entreprises ?

Contrairement à une Blockchain d'échange de crypto-monnaies, qui réunit des utilisateurs anonymes dans un réseau public (cas du bitcoin), une Blockchain pour entreprise est un réseau privé avec des autorisations, basé sur des identités connues et ne nécessitant pas de crypto-monnaies.

Pour mieux comprendre comment fonctionne une Blockchain pour entreprise et évaluer son potentiel dans une transformation des réseaux d'entreprise, vous devez connaître les quatre concepts essentiels sur lesquels elle se fonde, comme l'illustre la Figure 2-2.

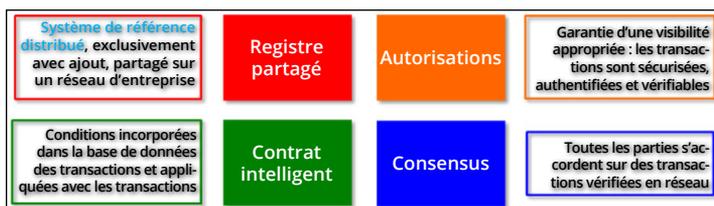


FIGURE 2-2 : Concepts clés d'une Blockchain pour entreprise.

Ces quatre concepts sont décrits dans cette section.

Registre partagé

Utilisés dans la comptabilité en partie double depuis le XIII^e siècle, les registres n'ont rien de nouveau. L'innovation réside dans le concept de registre partagé et distribué, fondé sur l'enregistrement immuable de toutes les transactions sur le réseau, visible par tous les membres du réseau. Avec un registre partagé, les transactions ne sont enregistrées qu'une seule fois, ce qui élimine toute redondance des actions, caractéristique des réseaux d'entreprise traditionnels. Un registre partagé possède les caractéristiques suivantes :

- » Il enregistre toutes les transactions effectuées sur le réseau d'entreprise ; le registre partagé est le système de référence, c'est-à-dire la source de fiabilité unique.
- » Il est partagé par tous les membres du réseau. Grâce à la duplication, chaque participant possède une copie de ce registre.
- » Il est assorti d'autorisations (privé), ce qui veut dire que les participants ne peuvent visualiser que les transactions qu'ils sont autorisés à voir. Les participants possèdent des identités qui les relient aux transactions, mais ils peuvent choisir les informations relatives aux transactions que d'autres participants sont autorisés à voir.

Autorisations

Une Blockchain peut être assortie d'autorisations ou non. Dans une Blockchain privée (*permissioned*), chaque membre possède une identité unique qui permet l'utilisation des politiques pour réguler la participation au réseau et accéder aux détails des transactions. Grâce à cette possibilité de réguler la participation, les entreprises et organisations peuvent plus facilement respecter leurs obligations légales de protection des données, notamment celles prévues par la réglementation HIPAA (Health Insurance Portability and Accountability Act, système de santé et d'assurance maladie des États-Unis). Les Blockchains privées sont également plus efficaces pour contrôler la cohérence des données ajoutées à la chaîne.

Grâce à la possibilité de restreindre l'accès aux détails des transactions, il est possible de stocker davantage d'informations dans la Blockchain et les participants peuvent définir les informations qu'ils souhaitent rendre visibles pour les autres. En outre, certains participants peuvent n'être autorisés à visualiser que certaines transactions. En revanche, d'autres, comme les chargés d'audit, peuvent avoir accès à un éventail plus large de transactions. (Dans une Blockchain publique, il est possible de limiter le niveau d'information accessible pour protéger la confidentialité et l'anonymat.)

À titre d'exemple, si la partie A transfère un actif vers la partie B, les deux parties peuvent visualiser les détails de cette transaction. La partie C peut voir que les parties A et B ont effectué une transaction, mais ne peut pas connaître les détails du transfert de cet actif. Si un chargé d'audit ou un intervenant d'un organisme de régulation rejoint le réseau, les services de confidentialité permettent de veiller à ce qu'ils puissent visualiser toutes les informations relatives aux transactions effectuées sur le réseau. C'est grâce à la technologie cryptographique — qui utilise des *certificats numériques* — qu'il est possible de gérer ces niveaux d'autorisation.

À l'instar d'un passeport, un certificat numérique contient des informations d'identification, empêche la falsification et peut être vérifié, car il a été émis par une agence digne de confiance. Un réseau Blockchain comporte une autorité de certification chargée d'émettre des certificats numériques.

Consensus

Dans un réseau d'entreprises dont les participants sont connus et dignes de confiance, les transactions peuvent être vérifiées et inscrites dans le registre par différents moyens de *consensus* (accord), en particulier de la manière suivante :

- » **Preuve de participation** : Pour valider les transactions, les validateurs doivent détenir un certain pourcentage de la valeur totale du réseau. Une preuve de participation peut assurer une protection accrue contre les attaques malveillantes du réseau en réduisant la motivation des attaquants et en fixant un coût élevé pour la mise en œuvre de l'opération.
- » **Signatures multiples** : Une majorité de validateurs (par exemple trois sur cinq) doivent s'accorder sur la validité d'une transaction.
- » **Règlement des litiges (tolérance aux divergences - PBFT)** : Un algorithme permet de régler les litiges entre *nœuds* informatiques (membres du réseau) lorsqu'un nœud d'un ensemble produit des informations différentes des autres.



À RETENIR

Une Blockchain d'entreprise peut utiliser le *consensus* « *intégrable* », qui permet d'appliquer le mécanisme de consensus le plus approprié pour un secteur d'activité particulier.

PREUVE DE TRAVAIL : UN INVESTISSEMENT SUPERFLU POUR UNE BLOCKCHAIN D'ENTREPRISE

Lorsque les participants sont anonymes (notamment dans l'environnement bitcoin), la mise en œuvre de transactions est coûteuse. Avec un réseau bitcoin, le consensus est obtenu grâce à des *preuves de travail*. Le réseau propose un problème à chaque machine possédant une copie du registre, en fonction de sa version du registre. Les machines possédant des exemplaires identiques du registre « s'associent » pour résoudre le problème qui leur est posé. La première équipe à résoudre le problème l'emporte et toutes les autres machines actualisent leur registre pour qu'il corresponde à celui de l'équipe gagnante. L'idée consiste à faire en sorte que la majorité l'emporte, car elle possède la plus grande puissance informatique pour résoudre le problème avant les autres.

Une preuve de travail est efficace dans une Blockchain publique, par exemple dans l'univers du bitcoin, mais elle absorbe une puissance informatique et une quantité d'électricité considérables, ce qui en fait une approche coûteuse pour réaliser le consensus. Cet investissement est inutile dans un réseau d'entreprises privé dont tous les participants sont connus.

Contrats intelligents

Un *contrat intelligent* est un accord ou un ensemble de règles régissant une transaction entre entreprises. Il est stocké dans la Blockchain et mis en œuvre automatiquement dans le cadre d'une transaction. Les contrats intelligents peuvent comporter différentes clauses contractuelles susceptibles d'être, en tout ou partie, directement applicables et/ou exécutoires de manière automatique. Leur finalité est d'apporter une sécurité supérieure, mais aussi de diminuer les coûts et les délais par rapport aux contrats traditionnels.

À titre d'exemple, un contrat intelligent peut définir les conditions contractuelles régissant le transfert d'un titre d'obligation d'entreprise. Il peut aussi définir les conditions générales d'une assurance voyage, qui peuvent être automatiquement applicables lorsque, par exemple, un vol est retardé de plus de six heures.

Identification et rôles des participants

Les différents membres d'un réseau Blockchain jouent un rôle dans son fonctionnement. Les descriptions qui suivent concernent chaque type de participant :

- » **Utilisateur de la Blockchain** : Participant (généralement un utilisateur au sein d'une entreprise) possédant les autorisations nécessaires pour rejoindre le réseau et effectuer des transactions avec d'autres participants. La technologie Blockchain fonctionne en arrière-plan, sans que les utilisateurs le sachent. Un réseau d'entreprise comporte généralement de nombreux utilisateurs.
- » **Agent de régulation** : Utilisateur Blockchain possédant des autorisations spéciales pour superviser les transactions effectuées au sein du réseau. Il est possible que les agents de régulation ne soient pas autorisés à effectuer des transactions.
- » **Développeur Blockchain** : Programmeur chargé de créer les applications et les contrats intelligents qui permettent aux utilisateurs Blockchain d'effectuer des transactions sur le réseau. Les applications servent de lien entre les utilisateurs et la Blockchain.
- » **Opérateur réseau Blockchain** : Personne possédant les autorisations spéciales et l'autorité nécessaire pour définir, créer, gérer et surveiller le réseau Blockchain. Toute entreprise utilisant un réseau Blockchain doit posséder un opérateur de réseau Blockchain.
- » **Plateformes de traitement traditionnelles** : Systèmes informatiques existants, susceptibles d'être utilisés par la Blockchain pour enrichir les traitements. Ces systèmes peuvent également avoir besoin de lancer des requêtes auprès de la Blockchain.
- » **Sources de données traditionnelles** : Systèmes de données existants capables de fournir des données pour influencer sur les modalités d'application des contrats intelligents. Ces données servent également à définir comment la communication et le transfert des données vont être effectués entre les applications/les données traditionnelles et la Blockchain. Ces systèmes peuvent utiliser des appels API et/ou des protocoles de messagerie cloud comme MQ.
- » **Autorité de certification** : Personne qui émet et gère les différents types de certificats requis pour faire fonctionner une Blockchain privée. À titre d'exemple, il peut être nécessaire d'émettre des certificats pour les utilisateurs d'une Blockchain ou pour des transactions individuelles.

- » Le potentiel d'une Blockchain pour éliminer les frictions commerciales
- » L'évolution vers des réseaux d'entreprises sans friction
- » La puissance de transformation qu'offre une visibilité plus large

Chapitre 3

Dynamiser l'entreprise avec la Blockchain

Si le commerce mondial a été le plus grand créateur de richesses de l'histoire de l'humanité, les *frictions commerciales* ont été leur frein le plus puissant. Au fil du temps, les entreprises ont résolu d'innombrables sources de friction. Pour réduire les risques liés aux transactions entre entreprises, des institutions et des instruments destinés à susciter la confiance ont été créés. De leur côté, les innovations technologiques ont contribué à rapprocher les interlocuteurs et à gagner en efficacité. Pour autant, la plupart des transactions professionnelles restent inefficaces, coûteuses et vulnérables.

La technologie Blockchain dispose du potentiel nécessaire pour éliminer ce qu'il reste de frictions commerciales, qui sont autant de freins au déroulement des activités. Avec la disparition des frictions va émerger une nouvelle science des organisations, capable de transformer en profondeur la manière dont les secteurs d'activité et les entreprises sont structurés. La transparence devenant la norme, une fondation robuste destinée à créer la confiance peut devenir un tremplin pour une nouvelle évolution des écosystèmes. Jusqu'ici écartés des marchés, certains participants et leurs actifs peuvent aujourd'hui se réunir en réseau en libérant un flux accéléré de capitaux pour créer de la richesse.

Identifier les types de frictions commerciales

La notion de friction commerciale correspond à tout ce qui peut freiner l'échange d'actifs. Il peut s'agir de coûts ou de délais supplémentaires, comme les taxes, la réglementation, la bureaucratie, la fraude, la nécessité d'intermédiaires, les délais d'application des contrats, etc. Les différents types de frictions rencontrées sur le marché influent de manière variable selon les secteurs d'activité, et à des degrés divers. Mais elles ont en commun de freiner le commerce mondial, en ralentissant, voire même en stoppant net, les activités. Vous découvrirez dans cette section les types de frictions commerciales les plus courants que la Blockchain peut atténuer.

Frictions relatives aux informations

Les *frictions relatives aux informations* découlent des limites suivantes :

- » **Informations imparfaites** : Les participants concernés par une transaction n'ont pas accès aux mêmes informations, ce qui donne un avantage déloyal à l'une des parties. Il est possible que les informations soient incorrectes ou incohérentes, ce qui conduit à de mauvaises décisions ou à des retards liés à la nécessité de les concilier.
- » **Informations inaccessibles** : La valeur potentielle des données et des informations disponibles en abondance est considérablement restreinte par les problématiques techniques que représentent le stockage, le traitement, le partage et l'analyse de ces connaissances. Conséquence : la plupart des informations ne sont ni collectées ni accessibles.
- » **Risques relatifs aux informations** : Les risques technologiques relatifs aux informations (piratage, cybercriminalité, confidentialité, vol d'identité) augmentent. Ce qui conduit à une augmentation des coûts, mais aussi à des atteintes à la réputation des marques.

Frictions relatives aux interactions

Les *frictions relatives aux interactions* augmentent lorsque le coût des transactions est trop élevé ou que le degré de séparation (physique ou autre) entre les parties est trop important. Certaines transactions entre professionnels nécessitent plusieurs jours et entraînent des coûts de gestion liés aux intermédiaires. Pour des concurrents plus agiles, ces transactions sont des cibles de choix.



À RETENIR

Les frictions relatives aux interactions sont souvent amplifiées par le nombre d'échanges requis. Avec son architecture de pair à pair, une Blockchain peut souvent réduire le nombre d'interactions ou de parties requises pour effectuer une transaction, ce qui réduit de fait le nombre de sources potentielles de frictions.

Frictions relatives à l'innovation

Les *frictions relatives à l'innovation* correspondent aux conditions, internes ou externes, qui freinent la capacité d'une entreprise ou d'une organisation à répondre aux évolutions du marché :

- » **Inertie institutionnelle** : La bureaucratie et les systèmes traditionnels internes, mais aussi la résistance naturelle des êtres humains au changement, peuvent diminuer la réactivité d'une entreprise.
- » **Restrictions liées à la réglementation** : La réglementation est bien sûr nécessaire pour contrôler le fonctionnement des différents secteurs d'activité, mais elle a pour conséquence d'introduire des coûts et des pertes de temps.
- » **Menaces invisibles** : Les nouveaux business models concurrentiels qu'apportent les nouvelles technologies sont des menaces imprévisibles pour les entreprises. Pour nombre d'entre elles, cette incertitude croissante va perturber la possibilité d'un succès durable de leurs activités. Qu'il s'agisse de petites entreprises ou d'entités économiques plus grandes et plus agiles, de nouvelles approches vont apparaître. Même si nombre d'entreprises échouent, certaines redéfiniront des secteurs d'activité tout entiers.

Évoluer vers des réseaux d'entreprises sans friction

Siècle après siècle, les innovations ont éliminé les sources de friction en réduisant les inefficacités qui freinaient le progrès. C'est ainsi, par exemple, que les premières lettres de crédit, au XIV^e siècle, ont établi de nouvelles bases pour susciter la confiance. Bien plus tard, l'invention du téléphone a permis les communications vocales en temps réel sur de grandes distances. Le réseau Internet, à son tour, a propulsé à la vitesse de la lumière ce qui n'était jusque-là qu'une lente approche destinée à dissiper les frictions. Spécialistes des technologies et économistes ont alors commencé à anticiper un monde où les frictions auraient disparu. En théorie, les frictions pourraient être « numériquement éliminées ».

Internet a effectivement réduit certaines d'entre elles, comme les coûts des transactions, par exemple. Pour autant, même si certaines formes d'imperfection des informations ont été corrigées, le problème n'a pas été complètement résolu. Certaines frictions latentes sont conséquentes. Bien évidemment, elles sont devenues un enjeu de concurrence entre start-up qui rivalisent pour capitaliser sur leur élimination.

Parallèlement, d'autres frictions se sont développées. À cet égard, les contradictions des réglementations internationales freinent la mondialisation. La prévention des nouvelles menaces, notamment les

cyberattaques, est coûteuse, et les reprises d'activité le sont encore plus. Les écosystèmes sont étouffés par différents intermédiaires toujours enclins à obtenir leur part du gâteau. Point positif, une nouvelle technologie, la Blockchain, promet d'éliminer, ou tout au moins de réduire significativement, ces frictions résiduelles.

Réduire les frictions relatives aux informations

Les incertitudes relatives aux informations nécessaires pour prendre des décisions métier constituent fréquemment un frein aux activités. Certaines caractéristiques de la Blockchain indiquent qu'elle permet de réduire les frictions relatives aux informations, notamment :

- » **Registre partagé** : La Blockchain se base sur un changement de paradigme : les informations ne sont plus détenues par un responsable unique, mais intégrées dans un historique partagé tout au long du cycle de vie d'un actif ou d'une transaction. Les parties peuvent valider les transactions et vérifier les identités et la propriété sans intermédiaires tiers. Toutes les informations concernées peuvent être partagées avec d'autres en fonction de leur rôle et de leurs autorisations d'accès.
- » **Autorisations** : Une Blockchain pour réseau d'entreprises peut être établie sous la forme d'un club dont l'accès est réservé à ses membres. Chacun des participants possède une identité unique et ils doivent tous répondre à certains critères pour effectuer des transactions. Les participants peuvent mener des transactions en toute confiance en sachant que la personne avec laquelle ils traitent est bien celle qu'elle prétend être.
- » **Cryptographie** : Un processus de chiffrement évolué, associé à des autorisations, garantit la confidentialité sur le réseau, ce qui évite tout accès non autorisé aux détails des transactions et dissuade toute activité frauduleuse.
- » **Consensus** : Le consensus permet de garantir que toutes les transactions sont validées avant d'être introduites dans la chaîne, et la Blockchain elle-même possède une forte résistance aux tentatives de falsification.

Atténuer les frictions relatives aux interactions

Une blockchain est particulièrement bien armée pour réduire les frictions relatives aux interactions, car elle élimine les obstacles entre participants au cours d'une transaction. Certaines caractéristiques de la Blockchain indiquent qu'elle permet de réduire les frictions relatives aux interactions, notamment :

- » **Registre partagé** : La propriété d'un actif peut être transférée entre deux membres quelconques du réseau et la transaction est enregistrée dans le registre partagé.
- » **Communication basée sur les états** : Aujourd'hui, pour communiquer, les banques utilisent une architecture de messagerie sécurisée comme SWIFT pour effectuer leur travail. Chaque banque gère donc l'état de la tâche effectuée localement. Avec une Blockchain, les banques peuvent envoyer des messages qui représentent l'état partagé de la tâche dans la chaîne, chacun des messages permettant la progression de la tâche à l'étape suivante du cycle de vie.
- » **Transactions de pair à pair (P2P)** : Dans une Blockchain pour réseau d'entreprise, les participants échangent directement les actifs, sans avoir à traiter la transaction au moyen d'intermédiaires ou d'un point central de contrôle, ce qui réduit les coûts et les délais qui en découlent.
- » **Consensus** : À la place des intermédiaires, la Blockchain utilise des algorithmes de consensus pour valider et autoriser les transactions. Les participants peuvent mener leurs activités à une vitesse plus proche de celle de leurs décisions métier.
- » **Contrats intelligents** : Les contrats intelligents éliminent les tracas et les délais inhérents aux conditions en les inscrivant dans la transaction. Grâce à ces contrats, la Blockchain établit les conditions selon lesquelles une transaction ou un échange d'actifs peut avoir lieu. Cette démarche met fin aux navettes incessantes de télécopies ou de courriers électroniques pour vérifier, réviser et signer les contrats.

Atténuer les frictions relatives à l'innovation

Les frictions relatives à l'innovation sont probablement les plus difficiles à résoudre par des moyens exclusivement technologiques. Cependant, la Blockchain peut y contribuer, dans les domaines suivants :

- » **Éliminer les coûts liés à la complexité** : L'augmentation de la complexité des activités d'une entreprise ou d'une organisation se traduit par une diminution du résultat. Les Blockchains disposent du potentiel nécessaire pour éliminer les coûts liés à la complexité, et au final, redéfinir les limites traditionnelles d'une entité.
- » **Réduire les coûts et les délais de mise en œuvre des processus réglementaires** : L'automatisation ne peut pas intégralement éliminer la gouvernance par la régulation, mais elle permet de réduire les coûts et de diminuer les délais liés aux processus réglementaires.
- » **Élargir les opportunités** : Une blockchain peut être, selon le cas, une aubaine ou un obstacle pour les entreprises. D'un côté, elle apporte la technologie qui leur permettra de développer des business models

inédits et compétitifs. Cependant, si certaines entreprises pourront ainsi redéfinir des secteurs d'activité tout entiers, d'autres échoueront.

Pour en savoir plus sur les approches permettant de réduire ou d'éliminer les frictions commerciales, consultez l'étude de l'IBM Institute of Business Value ici : ibm.biz/blockchainstudy.

Transformer les écosystèmes grâce à une visibilité plus large

En améliorant la visibilité, une Blockchain possède le potentiel nécessaire pour transformer des écosystèmes de fond en comble. Les chaînes logistiques sont des exemples de premier choix où le potentiel d'une Blockchain peut être appliqué à la transformation de secteurs d'activités tout entiers. Les actions initiales de mise en place d'une Blockchain peuvent avoir un impact rapide, même en ne transformant qu'une petite partie d'une chaîne logistique, par exemple les informations utilisées pour les activités d'importation. Si les terminaux d'importation recevaient les données de connaissance (contrat de transport maritime) plus tôt au cours du processus, ils pourraient préparer et réaliser leurs opérations plus efficacement et sans problèmes de confidentialité. La technologie Blockchain pourrait ainsi faire en sorte de rendre visibles, en temps quasi réel, les données nécessaires (par exemple l'heure de départ et le poids des conteneurs), mais sans partager d'informations à propos des propriétaires ou de la valeur de la cargaison. Conséquence : les coûts liés aux retards et les pertes résultant de documents papier manquants pourraient être évités.

À plus grande échelle, une Blockchain permettrait de mettre en place une plate-forme robuste et sécurisée d'opérations logistiques communes, en coordonnant un large éventail d'activités (partage d'espaces de réserve en entrepôt, optimisation de flottes de camions et de conteneurs d'expédition). Distributeurs et fabricants pourraient ainsi considérablement améliorer les prévisions de la demande et le renouvellement des stocks. De leur côté, les institutions financières, grâce aux antécédents détaillés de la fiabilité d'un fournisseur, pourraient augmenter leurs engagements de crédit, si cruciaux pour accompagner la croissance de l'activité. Les organismes de régulation pourraient aussi remonter jusqu'à l'origine des marchandises à partir des matières premières, permettant ainsi plus facilement d'identifier les articles contrefaits, mais aussi les fournisseurs de matières frelatées.

Le chapitre 4 propose quelques exemples de cas d'utilisation plus spécifiques de la technologie Blockchain.

- » Les différentes possibilités de mise en œuvre d'une Blockchain dans l'entreprise
- » La puissance de transformation transversale d'une Blockchain pour différents secteurs d'activité
- » Comment la Blockchain permettrait-elle de rationaliser les activités dans votre secteur ?

Chapitre 4

La Blockchain en action : Cas d'utilisation

L'une des approches les plus efficaces pour comprendre la Blockchain, prendre la mesure de son potentiel et déterminer si la démarche permettrait d'améliorer la manière dont votre entreprise fonctionne, consiste à examiner les cas d'utilisation possibles. Ce chapitre est destiné à présenter un certain nombre de situations correspondant à un large éventail de secteurs d'activité.



À RETENIR

Les cas d'utilisation présentés dans ce chapitre n'abordent que succinctement le potentiel de la technologie Blockchain. Cette liste ne cessera de s'élargir proportionnellement à la maturité progressive de cette technologie. Pour découvrir les exemples les plus récents de cas d'utilisation, rendez-vous sur la page www.ibm.com/blockchain/for-business.html.

Services financiers

Le secteur des services financiers permet d'illustrer un certain nombre d'exemples d'utilisation de la Blockchain.

Financement professionnel

Les entreprises ont besoin d'ouvrir des crédits pour acheter des biens et des services, avec une visibilité de bout en bout pour éviter et résoudre les litiges relatifs aux transactions. À titre d'exemple, IBM Global Financing (IGF) propose, dans le monde entier, des offres de financement à ses partenaires pour leur permettre d'acquérir des biens et des services

auprès de fournisseurs au moyen de crédits approuvés par IBM. Avec plus de 4 000 partenaires et fournisseurs qui utilisent tous des systèmes différents et souvent incompatibles, IBM a décidé de transférer la totalité des informations nécessaires dans une Blockchain et de la proposer aux utilisateurs sous la forme d'un registre distribué.



ASTUCE

Les avantages de cette mise en place sont les suivants :

- » Visibilité complète du pipeline, de la commande à la livraison.
- » Réduction du nombre de dossiers de contentieux déposés.
- » Réduction du délai nécessaire pour résoudre les dossiers de contentieux.

Finance pour le commerce international

Les entreprises ont besoin de rationaliser le processus d'obtention des approbations pour différentes entités légales (douanes, autorités portuaires, firmes de transport routier ou ferroviaire, etc.) liées au mouvement des marchandises dans le monde entier. La Blockchain peut donc être utilisée par ces entités légales pour signer toutes les approbations. De plus, elle permet de tenir informées toutes les parties concernées de l'état d'avancement des autorisations, et d'indiquer quand les marchandises sont reçues et le règlement transféré de la banque de l'importateur vers celle de l'exportateur.



ASTUCE

Les avantages de la démarche pour le financement des opérations de commerce international sont les suivants :

- » Simplification des processus complexes pour ne garder qu'un processus unique, et ce, en accédant à un registre intermédiaire.
- » Accès plus efficace aux capitaux, débarrassé des longs délais de règlement, des erreurs et des litiges.
- » Confiance accrue et engagement responsable des entreprises, des organismes de régulation et des consommateurs.

Transactions internationales

Les banques ont besoin d'une démarche pour gérer leurs comptes *nostro/vostro*. *Nostro* (notre) fait référence à un compte détenu par une banque dans une autre banque située à l'étranger, tenu en devise du pays étranger. *Vostro* (votre) précise comment la banque située dans un pays étranger fait référence à ce compte. Ces comptes servent à faciliter et à simplifier les transactions de commerce et d'échange avec l'étranger par des opérations de rapprochement. Les comptes *nostro/vostro* peuvent prendre la forme de transactions de comptes stockées dans une

Blockchain, ce qui permet d'améliorer considérablement la transparence et l'efficacité par un rapprochement automatisé des comptes.



ASTUCE

Les avantages sont les suivants :

- » Possibilité de gérer les transactions pour l'ensemble des comptes vostro/nostro d'une banque au moyen d'une interface unique.
- » Visibilité accrue de l'état des transactions, des soldes et du suivi dans le temps.
- » Vision exacte, cohérente et permanente de l'ensemble des comptes nostro/vostro.

Assurance

Le secteur de l'assurance peut également utiliser la démarche Blockchain.

Les compagnies d'assurances ont besoin d'une approche efficace pour traiter les dossiers, vérifier la réalité d'un événement assurable (par exemple, un accident) et proposer au client une indemnisation équitable et rapide. Grâce au traitement automatisé des dossiers d'assurance, les conditions des polices d'assurance sont stipulées dans un contrat intelligent, stocké dans la Blockchain, et relié à des données disponibles publiquement sur Internet. Lorsqu'un événement assurable se produit et est signalé par une source digne de confiance, la police d'assurance est automatiquement déclenchée. Le dossier est ensuite traité en fonction des conditions spécifiées dans le contrat intelligent, et le client reçoit son indemnisation.



ASTUCE

Les avantages pour le secteur de l'assurance sont les suivants :

- » Élimination des coûts de traitement des dossiers d'assurance.
- » Réduction des possibilités de fraude à l'assurance.
- » Amélioration de la satisfaction des clients.

Administration publique

Une proportion considérable des activités de l'administration publique concerne la consignation de transactions et le suivi des droits. Ces opérations peuvent être plus efficaces et transparentes en utilisant une Blockchain.

Établir l'authenticité d'une identité reste un problème du fait de la possibilité de falsifications et du montant des coûts des vérifications. Il est possible que des millions de personnes dans le monde aient falsifié leurs

papers d'identité et ne soient pas véritablement celles qu'elles prétendent. De plus, des millions de réfugiés et leurs enfants ne disposent d'aucun papier d'identité. Les habitants des pays les plus pauvres de la planète ne disposent pas nécessairement de preuves suffisantes pour établir leur identité, comme le demandent certains fournisseurs de services. À titre d'exemple, les banques exigent généralement un justificatif de domicile ou des factures d'eau ou d'électricité pour établir une identité, et ces informations ne sont pas toujours disponibles dans les pays en voie de développement.

Les organismes concernés peuvent utiliser la Blockchain en produisant des certificats de naissance numériques authentifiés, infalsifiables, horodatés et accessibles à tous, partout dans le monde. Les avantages de la démarche sont les suivants :

- » Réduction des coûts et des délais de vérification des identités.
- » Réduction du trafic des êtres humains.
- » Transparence dans l'attribution des subventions.

Gestion de la chaîne logistique

Lorsque quelque chose ne fonctionne pas correctement dans un « système de systèmes » complexe, par exemple un avion, il est essentiel de connaître, grâce à un outil de gestion de la chaîne logistique, la provenance de chaque composant, avec des précisions comme le nom du constructeur, la date de production, le lot et même le programme de la machine utilisée pour la fabrication.

Un réseau Blockchain permet ainsi de tenir à jour les informations détaillées relatives à la provenance de chaque pièce, accessibles pour les fabricants participant au processus de production, mais aussi pour les sociétés propriétaires des avions, les entreprises chargées de la maintenance et les autorités de régulation officielles.



ASTUCE

Les avantages de la démarche pour ce domaine sont les suivants :

- » Confiance accrue, car les informations ne sont « détenues » par aucune autorité unique.
- » Gains d'efficacité qui permet de réduire les délais nécessaires pour diagnostiquer et résoudre un défaut, ce qui permettra d'améliorer l'exploitation du système.
- » Rappels ciblés plutôt que génériques et à l'échelle de l'ensemble d'une flotte.



SUR LE WEB

La notion de provenance est également essentielle pour les chaînes logistiques alimentaires. Pour découvrir comment la Blockchain peut s'inscrire dans une démarche d'amélioration de la traçabilité des chaînes logistiques alimentaires, rendez-vous sur la page <http://ibm.biz/FoodSupplyChain>.

Santé

Le secteur de la santé a besoin de systèmes plus efficaces et sécurisés pour pouvoir gérer les dossiers médicaux des patients, les accords préalables de paiement, le règlement des dossiers d'assurance, et la mise en œuvre et l'enregistrement d'autres transactions complexes. D'où l'intérêt de la Blockchain d'apporter à ce secteur les moyens dont il a tant besoin.

Dossiers médicaux personnels

Les dossiers médicaux de patients sont actuellement gérés dans des centres de données (avec des environnements de type cloud). L'accès est limité aux réseaux des établissements hospitaliers et des prestataires de soins. La centralisation de ces informations, très coûteuse, les rend vulnérables aux atteintes à la sécurité.

En revanche, une Blockchain mémorise l'ensemble de l'historique médical de chaque patient, avec différents niveaux de contrôle selon l'intervenant (patients, médecins, organismes régulateurs, établissements hospitaliers, assureurs, etc.). Il s'agit donc d'un mécanisme sécurisé qui permet de stocker et gérer le dossier médical complet d'un patient.

Compte tenu de ces éléments, les avantages de la démarche pour ce secteur sont les suivants :



ASTUCE

- » Moyens de stockage protégés contre les falsifications des antécédents médicaux.
- » Réduction des délais de résolution des dossiers d'assurance et gains d'efficacité pour la production d'une offre d'assurance.
- » Historique médical complet du patient destiné aux médecins pour la prescription précise de médicaments.

Accords préalables de paiement

La notion de « documents cliniques complémentaires » recouvre la nécessité d'apporter des informations cliniques supplémentaires pour permettre à un organisme payeur de statuer sur un dossier de santé. Ces dossiers sont souvent déposés sans l'ensemble des informations requises, ce qui oblige les organismes payeurs à demander de nouvelles

informations, contribuant ainsi à accroître les coûts et les délais de règlement. En outre, corréler les dossiers et les informations nécessaires pose un problème pour toutes les parties concernées.



ASTUCE

La Blockchain peut simplifier ce processus compliqué et fastidieux en automatisant la collecte et le partage des informations. Les autres avantages de la démarche sont les suivants :

- » Il est possible d'examiner et de régler les dossiers de manière plus efficace et rapide.
- » Le système peut suggérer d'autres offres de services dont la couverture est plus performante.

Internet des objets (IoT)

Au fil de leurs échanges mutuels, les machines peuvent signaler les interactions pertinentes et les enregistrer dans la Blockchain pour améliorer l'efficacité et la précision, et réduire les coûts. Les applications de logistique commerciale utilisent la Blockchain pour automatiser les processus relatifs à l'Internet des objets.

La logistique de fret, par exemple, concerne différentes parties : fabricants, transitaires, expéditeurs, douanes et assureurs. Bien qu'elles interagissent et dépendent souvent les unes des autres, ces parties peuvent avoir des objectifs distincts et utiliser des systèmes différents pour le suivi des cargaisons. Dans ce contexte, une Blockchain IoT sert de registre partagé pour enregistrer les conteneurs d'expédition au fur et à mesure de leur progression dans le système. Il est possible d'actualiser les contrats intelligents de manière automatique à l'aide de l'IoT Foundation et de les optimiser pour mettre en œuvre, avec la Blockchain, des échanges commerciaux internationaux intégrant l'IoT.



ASTUCE

La démarche offre les avantages suivants :

- » La plus grande transparence du suivi des expéditions permet de gagner en efficacité.
- » Le niveau de confiance est plus élevé, car toutes les transactions sont enregistrées de manière indélébile.
- » La démarche permet de gagner en fiabilité et les coûts sont réduits grâce à la contribution de la technologie IoT.
- » Les participants peuvent optimiser et automatiser les processus métier grâce aux capacités de l'IoT.
- » Les prévisions futures permettent d'imaginer le principe d'un « fret autonome ».

- » Découverte des principes de l'Hyperledger
- » Différences entre Hyperledger et Hyperledger Fabric
- » Ce que peut apporter IBM pour aider les développeurs à innover avec la Blockchain

Chapitre 5

Hyperledger, projet de la Linux Foundation

Projet de la Linux Foundation, Hyperledger est une communauté open source destinée à contribuer à l'évolution technologique et à la réflexion stratégique. Elle peut être vue comme une plateforme destinée à accueillir des communautés de développeurs dont l'objectif est de construire des Blockchains open source et leurs technologies associées. C'est en décembre 2015 que la plateforme Hyperledger a été annoncée et son nom choisi par 17 entreprises. L'objectif était de collaborer pour contribuer à l'évolution et à l'utilisation de la technologie Blockchain dans les différents secteurs d'activité de l'entreprise. Avec 130 membres dans le monde entier, il s'agit aujourd'hui du projet le plus dynamique de l'histoire de la Linux Foundation.



À RETENIR

Le projet Hyperledger est géré par la Linux Foundation, qui apporte les outils, les formations et les événements nécessaires pour développer des projets open source. IBM a contribué au projet initial, baptisé *Open Blockchain*, devenu aujourd'hui *Fabric*. Il s'agit sans doute du projet le plus large et ambitieux. Intel a contribué au projet avec sa plateforme « Sawtooth Lake », technologie de Blockchain avec laquelle a été introduit le consensus PoET (Proof of Elapsed Time). Parmi les autres projets notables figurent « Iroha » (plate-forme Blockchain C++) et « Cello » (déploiement rapide de Blockchain sur des plates-formes cloud). Plutôt que de jouer le rôle de plate-forme unique (de type Ethereum), Hyperledger se rapproche davantage du Projet Apache. Il s'agit de réunir différents projets sur une plate-forme cadre open source, disponible librement et possédant, dans l'idéal, un certain nombre de règles

d'interopérabilité. Pour en savoir plus sur la théorie de la plate-forme Hyperledger, rendez-vous sur la page <http://ibm.biz/UmbrellaHyperledger>.

Les perspectives d'Hyperledger

L'idée sous-jacente d'Hyperledger est de proposer des éléments standardisés robustes et efficaces de technologie Blockchain, destinés à faciliter l'adoption et la banalisation de la démarche. Les applications futures s'inscrivent dans un environnement formé de nombreuses bases de données et Blockchains distribuées et interconnectées, mais spécialisées pour répondre aux besoins de leurs utilisateurs. Elles seront en outre, le cas échéant, en mesure de communiquer avec d'autres registres.

Autre objectif de la plate-forme Hyperledger, proposer une technologie Blockchain modulaire dotée d'une interface de programmation des applications (API) conviviale et de nombreux modules spécifiques permettant un développement facile et apportant de l'interopérabilité. L'API doit bénéficier d'une flexibilité suffisante pour permettre de construire des Blockchains en dehors du noyau Hyperledger, permettant ainsi des interactions faciles avec leurs composants et avec les Blockchains.

HYPERLEDGER ET HYPERLEDGER FABRIC : QUELLE DIFFÉRENCE ?

Hyperledger est une démarche collaborative open source de la Linux Foundation destinée à créer une technologie de Blockchain adaptée à l'entreprise. *Hyperledger Fabric* est un framework de Blockchain et l'un des projets Hyperledger hébergés par la Linux Foundation. Il bénéficie d'une architecture modulaire de services intégrables et interchangeables utilisant la technologie des conteneurs.

- Adapté à un large éventail de cas d'utilisation sectoriels, caractérisés par des exigences variées.
- Conformité avec les législations et réglementations existantes.
- Prise en compte des identités vérifiées et des transactions privées et confidentielles.
- Prise en compte des registres partagés privés.
- Gestion des performances, de l'évolutivité, de la contrôlabilité, des identités et de la confidentialité.
- Réduction des traitements coûteux relatifs aux preuves de travail.

En outre, Hyperledger considère qu'il doit être difficile pour des membres non autorisés de certifier l'identité et les profils de comportement d'un membre quelconque du réseau en inspectant le registre. Les utilisateurs d'une Blockchain doivent pouvoir assurer la confidentialité de certaines informations relatives aux transactions (logique métier, paramètres), en les rendant inaccessibles à d'autres personnes que les participants.

Hyperledger Fabric

Hyperledger Fabric offre un framework destiné au développement de solutions de Blockchain avec une architecture modulaire, des implémentations intégrables et une technologie utilisant les conteneurs. Tout en s'appuyant sur les meilleures pratiques open source, Hyperledger Fabric apporte confidentialité, évolutivité et sécurité dans les environnements métier.

Contrairement à d'autres configurations Blockchain comme la crypto-monnaie Bitcoin ou l'environnement Ethereum, Hyperledger Fabric possède les quatre éléments clés d'une Blockchain pour l'entreprise :

- » **Réseau privé** : Qualité de membre et droits d'accès définis collectivement dans votre réseau d'entreprise.
- » **Confidentialité des transactions** : Apporte aux entreprises la flexibilité et la sécurité nécessaires pour donner de la visibilité aux transactions pour des parties spécifiques possédant les bonnes clés de cryptage.
- » **Pas de crypto-monnaies** : Ne nécessite ni « mining », ni traitements coûteux pour effectuer des transactions.
- » **Programmable** : Utilise la logique incorporée dans les contrats intelligents pour automatiser les processus métier dans l'ensemble de votre réseau.

Membre fondateur du projet Hyperledger, IBM a fait don de 44 000 lignes de code blockchain dans le cadre de l'initiative Hyperledger Fabric. En outre, IBM :

- » S'inscrit dans une approche élargie, transversale aux secteurs d'activité et open source pour développer le potentiel de la Blockchain et banaliser l'approche.
- » Considère que l'environnement Hyperledger va libérer les développeurs dans tous les secteurs d'activité en leur apportant les moyens de se focaliser sur la création d'applications et de plateformes robustes, capables de prendre en compte des types de transactions métier très différents sur Internet.

» A réalisé des investissements considérables en recherche et développement pour explorer les applications de Blockchain pour l'industrie et a fait don de son code et de ses droits de propriété intellectuelle.



À RETENIR

Pour réaliser pleinement le potentiel de la Blockchain, il est essentiel de mettre en place une approche basée sur des standards ouverts, ce qui permettra l'adoption massive de la démarche et l'éclosion d'innombrables innovations.



ASTUCE

Rendez-vous sur le site Hyperledger Rocket Chat Channel à l'adresse chat.hyperledger.org et rejoignez une communauté dynamique de plus de 5 000 développeurs qui construisent déjà leurs applications grâce aux technologies Hyperledger.

Que peut apporter IBM pour aider les développeurs à innover avec la Blockchain ?

IBM libère le potentiel de la Blockchain en la rendant plus accessible et ouverte. Situé parmi les structures de recherche les plus performantes du monde, IBM s'est fixé pour objectif d'explorer de nouvelles approches contribuant à l'évolution de la science de la Blockchain en éliminant en partie sa complexité et en lui apportant accessibilité et ouverture.

Un environnement cloud et une plateforme de développement facilement accessibles

Pour démarrer le plus rapidement possible, le cloud IBM est l'approche la plus simple pour mettre en œuvre vos solutions Blockchain. IBM propose un certain nombre de solutions Cloud pour vous permettre de développer facilement des applications tout en testant la sécurité, la disponibilité et les performances d'un réseau Blockchain privé.



À RETENIR

Les réseaux Blockchain d'IBM sont conçus pour tirer le meilleur parti d'un contrôle décentralisé, même si certains environnements cloud sont sensibles aux vulnérabilités. En associant plusieurs équipes d'experts de la sécurité, de spécialistes de la cryptographie, d'experts du matériel et de chercheurs, IBM a créé des services cloud essentiels sur lesquels peuvent s'appuyer des réseaux Blockchain dignes de confiance et protégés contre les falsifications.

IBM Blockchain on Bluemix

Grâce au service Blockchain sur Bluemix, vous pouvez créer et déployer un réseau Blockchain basé sur la plateforme Hyperledger Fabric. IBM Blockchain sur Bluemix propose un programme hautement sécurisé, caractérisé par un environnement isolé destiné aux réseaux d'entreprise.

Il permet d'étendre les fonctionnalités initiales de base au sein d'un environnement isolé intégré à une infrastructure sécurisée. Ce programme s'accompagne de niveaux élevés de sécurité permettant de bloquer les portes dérobées (ou *backdoors*) pour éviter les accès non autorisés et les falsifications. Les caractéristiques essentielles de ce programme sont les suivantes :

- » L'environnement d'exploitation de la Blockchain protège les administrateurs de l'hôte et produit des preuves pour veiller à ce que la Blockchain fonctionne selon les conditions définies.
- » Le niveau élevé d'assurance d'évaluation permet la protection de tous les environnements où les membres d'une Blockchain effectuent des transactions de manière isolée par rapport à d'autres membres et parties. Cette approche permet d'éviter toute fuite d'information vers l'environnement d'une autre partie.
- » L'optimisation des algorithmes cryptographiques s'appuie sur un environnement qui transfère les opérations de hachage et la création des signatures numériques vers des accélérateurs optimisés qui n'absorbent aucune puissance de calcul de l'unité centrale.
- » La norme FIPS 140-2 (spécification la plus exigeante des normes fédérales de traitement de l'information) prévoit l'utilisation de la Blockchain dans des secteurs d'activité régulés, notamment l'administration publique, les services financiers et la santé.



SUR LE WEB

Pour en savoir plus sur les options IBM Blockchain on Bluemix, rendez-vous sur la page www.ibm.com/blockchain/offerings.html.

Images Hyperledger Fabric sur DockerHub

À titre de variante, vous pouvez extraire directement des images Hyperledger Fabric de Docker Hub pour créer et gérer votre propre réseau Blockchain local. Vous pouvez également installer et mettre en œuvre un réseau Blockchain avec les scripts et les images Docker Compose certifiés IBM. Pour en savoir plus sur l'approche nécessaire pour démarrer, rendez-vous sur la page <http://ibm.biz/QuickStartGuide>.



ASTUCE

Une fois votre réseau déployé, vous êtes prêt à construire votre premier chaincode (code de chaîne) ! Pour obtenir votre badge de chaincode, suivez cette formation : <http://ibm.biz/BlockchainChaincodeCourse>.

Analyse individualisée et expertise sectorielle

Si vous êtes parvenu à ce point, vous êtes sans doute impatient de bâtir à partir d'une démarche Blockchain. Il vous faudra donc être épaulé pour proposer à d'autres membres de votre structure de rejoindre le réseau. C'est justement la finalité de cette section.



ASTUCE

IBM développe un certain nombre de solutions Blockchain pour des clients opérant dans différents secteurs d'activité. IBM Bluemix Garage for Blockchain est un atelier collaboratif grâce auquel vous pouvez explorer les cas d'utilisation d'une Blockchain. Vous pouvez ainsi déterminer votre premier pilote le plus performant avec cette technologie.

Le modèle d'approche d'IBM Bluemix Garage for Blockchain se décompose en trois étapes :

- » **Entretien et démonstration** : Une session interactive de 90 minutes réunissant les membres de l'équipe IBM Bluemix Garage for Blockchain et le client. Il est préférable de prévoir une session en face à face, mais il est également possible d'organiser une conférence en ligne, une vidéoconférence ou un entretien téléphonique. IBM présente son point de vue sur la Blockchain dans des termes compréhensibles par l'entreprise et en évitant tout jargon technique. La discussion se poursuit avec les apports de la Blockchain pour votre entreprise, suivis d'une démonstration succincte, interactive et immédiate d'un cas d'utilisation (voir le chapitre 4 qui contient quelques cas d'utilisation donnés à titre d'exemple).
- » **Aspects pratique de la technologie** : Cet atelier d'une journée, en face à face et extrêmement interactif, permet de découvrir de manière plus détaillée la technologie Blockchain. En associant présentations et exercices pratiques guidés, IBM vous permet de découvrir tous les détails que vous souhaitez connaître pour exploiter pleinement la technologie Blockchain.
- » **Premier projet** : Le premier projet commence par un atelier IBM Design Thinking de deux jours, avec les spécialistes d'IBM, pour explorer le cas d'utilisation du point de vue de l'utilisateur. IBM conçoit ensuite un processus de développement agile itératif d'une solution bien circonscrite pour résoudre la problématique métier (cas d'utilisation). Cette solution est ensuite réalisée en mettant en œuvre un certain nombre de sessions de développement agile succinctes. Ces sessions sont en principe menées par une équipe conjointe de taille limitée (IBM Bluemix Garage for Blockchain + client), ce qui permet de combiner notre expertise de la Blockchain et du développement agile avec les connaissances du client concernant le cas d'utilisation et le scénario métier.

Les entreprises commencent à travailler autour de la stratégie, la planification et la mise en œuvre d'une démarche Blockchain. IBM Global Business Services (GBS) propose donc l'intervention d'équipes de consultants chevronnés dans le monde entier pour répondre à vos questions et commencer à organiser vos premiers projets.

- » Localiser les domaines où la Blockchain produit la meilleure rentabilité
- » Choisir un cas d'utilisation pertinent et en définir les objectifs
- » Identifier une plate-forme pour construire votre première application
- » Créer une communauté robuste avec les autres membres

Chapitre 6

Les 10 étapes clés de votre première application Blockchain

Après avoir découvert la puissance de transformation potentielle de la Blockchain pour l'entreprise, vous êtes probablement impatient de connaître les différentes étapes nécessaires pour aller vers sa mise en œuvre dans votre entreprise et votre secteur d'activité. Eh bien, vous êtes au bon endroit. Cette partie du livre est consacrée aux 10 étapes clés de votre première application Blockchain.

Décider si la Blockchain a sa place dans votre secteur d'activité

En avançant dans votre connaissance de la Blockchain, vous allez probablement découvrir son impact sur votre secteur d'activité. De plus, certaines de ses applications vous sembleront certainement aussi évidentes que celles qui vous permettent de résoudre vos problématiques actuelles. Si vous n'êtes pas certain de l'adéquation de la Blockchain avec votre secteur d'activité, posez-vous les questions suivantes :

- » Mon réseau d'entreprise a-t-il à gérer des relations contractuelles ?
- » Avons-nous besoin d'effectuer un suivi des transactions qui concernent plus de deux parties ?

- » Le système actuel est-il trop complexe ou coûteux, éventuellement du fait de la nécessité d'intermédiaires ou d'un point de contrôle central ?
- » Le réseau peut-il bénéficier d'une confiance accrue, d'une plus grande transparence et d'un engagement responsable plus important pour la gestion des informations ?
- » Le système existant est-il une source d'erreurs du fait des processus manuels ou de la redondance des actions ?
- » Le système de gestion des transactions existant est-il vulnérable aux actions frauduleuses, aux cyberattaques et aux erreurs humaines ?

Si la réponse à l'une de ces questions est oui, il est probable que la Blockchain convienne à votre secteur d'activité.

Identifier les freins aux processus métier

Examinez vos processus métier actuels. Repérez les inefficacités, en particulier les étapes générant des retards, des déceptions, des erreurs et des actions redondantes. Il est probable que les questions de la section précédente vous mettent sur la piste.



ASTUCE

Vous pouvez aussi vous poser une question plus générale : « Quels sont les défis auxquels j'ai actuellement à faire face dans mes réseaux de gestion des transactions ? »

Déterminer ce que peut vous apporter la Blockchain

Après avoir identifié les problématiques que vous rencontrez avec vos réseaux de gestion des transactions, vous pouvez examiner les différentes caractéristiques de la Blockchain qui vont vous permettre de répondre, entre autres, aux problèmes d'inefficacité et de coût. Par exemple, si l'absence de confiance introduit des frictions dans les transactions, le registre partagé de la Blockchain va vous permettre de gagner en visibilité sur les transactions et les historiques relatifs aux actifs pour accroître la confiance. Si les accords ou les règles métier introduisent des délais supplémentaires, il est possible que les contrats intelligents constituent la bonne solution. L'objectif, ici, consiste à déterminer comment la Blockchain peut vous aider à résoudre des problématiques spécifiques.

Choisir un cas d'utilisation approprié

Lorsque vous choisissez un cas d'utilisation, veillez à ce qu'il s'adapte parfaitement à ce que vous essayez de réaliser. Il doit s'agir d'une utilisation qui apporte réellement de la valeur ajoutée plutôt qu'une démarche qui pourrait être tout aussi bien menée avec une technologie déjà parvenue à maturité. Votre cas d'utilisation doit donc franchir les quatre tests décisifs suivants :

- » **Consensus** : Est-ce qu'un accord à l'échelle du réseau d'entreprise précisant que chaque transaction est valide constitue pour vous un avantage ?
- » **Provenance** : La gestion d'un historique complet est-elle importante pour vous ?
- » **Immuabilité** : Est-il important pour vous que la série de transactions comporte des témoins d'intégrité ?
- » **Finalité** : Avez-vous besoin d'un « système de référence » convenu avec les autres membres dans le réseau d'entreprise ?



ASTUCE

Essayez de choisir un cas d'utilisation moins complexe du point de vue organisationnel pour ne pas être submergé par la complexité lors de votre première découverte d'une Blockchain.

Déterminer la finalité de votre réseau Blockchain

Une fois le cas d'utilisation approprié choisi, définissez un objectif clair et mesurable pour votre premier projet. Que souhaitez-vous résoudre ou améliorer grâce à la technologie Blockchain ? Comment pouvez-vous évaluer la réussite de votre premier projet après avoir réalisé cet objectif ?

Souhaitez-vous réduire les délais de résolution des litiges ? Accélérer le traitement des dossiers ? Fluidifier votre flux de capitaux ? Réduire la fraude au sein de votre réseau ? Ces aspects ne sont que quelques-uns des objectifs possibles réalisables avec une Blockchain.

Identifier les dépendances

Lorsque vous avez réfléchi à un cas d'utilisation pertinent, réfléchissez aux autres éléments dont vous avez besoin, en plus des ressources internes que vous possédez déjà, pour lancer votre premier projet Blockchain. Ai-je besoin d'un partenaire de services pour déployer plus efficacement mon premier projet ? Avez-vous besoin d'une plateforme ou d'une structure qui vous permette de répondre à certaines obligations de conformité ou légales ? Le traitement des transactions devient un sport d'équipe. En effet, un réseau Blockchain est bien plus efficace lorsque différentes parties y participent, et l'efficacité et la création de valeur augmentent au fil du développement du réseau. Les entreprises ont besoin de découvrir un nouveau modèle de processus basé sur les écosystèmes. Il est donc essentiel de se lancer dès maintenant dans la démarche.

Choisir un fournisseur et une plateforme de Blockchain

Choisissez un fournisseur et une plateforme parfaitement adaptés à votre secteur d'activité et aux besoins de votre entreprise. En comparant l'adéquation de plusieurs fournisseurs et plateformes, essayez de répondre aux questions suivantes :

- » Avez-vous besoin d'un réseau privé ?
- » Devez-vous connaître les identités de chacun des membres de votre réseau d'entreprise ? Par exemple, pour respecter les obligations légales, notamment les réglementations anti-blanchiment (AML) ou Know your customer (KYC) pour connaître l'identité de vos clients ?
- » Avez-vous fréquemment des échanges avec d'autres personnes qu'il serait possible d'automatiser et de préprogrammer, libérant ainsi des ressources et un temps précieux pour d'autres activités ?
- » Selon vous, résoudre les transactions en quelques minutes plutôt que d'attendre plusieurs jours, voire plusieurs semaines, est-il un avantage ?

Pour repérer plus facilement une plateforme adaptée à vos besoins, consultez les options proposées au chapitre 5.

Développer et déployer le chaincode

L'étape suivante de votre premier projet Blockchain consiste à développer et à déployer une application et un réseau Blockchain.



SUR LE WEB

Pour connaître la méthode permettant de configurer un réseau Blockchain et de commencer à écrire le code, consultez le document << IBM Blockchain 101: Quick-start guide for developers >> à l'adresse <http://ibm.biz/QuickStartGuide>.

Tester et configurer votre application et votre réseau

L'étape finale de la création et du déploiement de votre première application Blockchain consiste en réalité à faire fonctionner le processus en continu. Surveillez votre application et votre réseau, puis tirez-en des enseignements pour y apporter des améliorations et envisager un déploiement plus large.



SUR LE WEB

Pour en savoir plus et accéder à des documentations relatives aux méthodes de test de votre réseau Blockchain, rendez-vous sur la page <http://ibm.biz/TestNetwork>. Le moniteur de tableau de bord est un outil intéressant pour le déploiement et le test de votre réseau Blockchain. Pour en savoir plus sur cet outil, rendez-vous sur la page <http://ibm.biz/DashboardMonitor>.

Participer à la plate-forme Hyperledger Rocket Chat Channel



SUR LE WEB

Rendez-vous sur le site Hyperledger Rocket.Chat Channel à l'adresse chat.hyperledger.org et rejoignez une communauté dynamique qui construit déjà ses applications grâce aux technologies Hyperledger. Vous y obtiendrez les réponses à toutes vos questions tout en construisant votre réseau. Vous pourrez aussi dialoguer avec vos pairs et vous intégrer pleinement à la communauté, alors que les technologies de Blockchain Hyperledger continuent d'évoluer.

Notes

Notes

Notes

Redéfinir vos réseaux d'entreprise avec la Blockchain

Le livre *La Blockchain pour les Nuls*, Édition limitée IBM, va vous permettre de découvrir la Blockchain, son fonctionnement et de quelle manière elle peut enrichir vos réseaux d'entreprise. Vous pourrez aussi découvrir comment cette technologie innovante peut s'appliquer dans votre secteur d'activité et comment vous pouvez dès aujourd'hui commencer à construire un réseau Blockchain.

À l'intérieur...

- Comprendre ce qu'est la Blockchain (et ce qu'elle n'est pas)
- Découvrir le potentiel de la Blockchain pour l'entreprise
- Appliquer la Blockchain à différents secteurs d'activité
- Découvrir le projet Hyperledger et le framework Fabric
- Construire votre première application



Manav Gupta est directeur technologique d'IBM Cloud Canada, auteur de livres pour l'édition, IBM Master Inventor, membre de l'IBM Academy of Technology et titulaire de la certification IBM Senior Certified IT Architect. Il a conduit de nombreux projets d'innovation en Amérique du Nord dans le domaine du cloud, du Big Data et, plus récemment, de la Blockchain.

Visitez le site
Dummies.com[®]

pour
les nuls[®]

ISBN: 978-1-119-48446-2
Référence : XIM12354-FRFR-00
Revente interdite

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.