

Whitepaper

IoT et Blockchain combinés: Quels sont les Usages?



Biographie des auteurs



Serge Bonnaud

Ingénieur diplômé de l'Epita et licencié en mathématiques, Serge Bonnaud a travaillé dans le domaine de l'ingénierie système pour la Défense (système d'armes tactique marine). Il a ainsi occupé différents postes chez des éditeurs de logiciel dont Verilog, IDE, Thomson Software Product et Rational Software Corporation. Il a été impliqué sur des projets dans le domaine de l'industrie de la santé, avec le développement de systèmes d'analyse biologique de données médicales ou l'optimisation de programmes multimédia.

Serge a rejoint IBM en 2004 où il a occupé des fonctions de Market Manager sur les solutions de production informatique puis Software Architect sur l'Afrique du Nord (IBM Maroc, Algérie, Tunisie).

Il a intégré en 2016 l'équipe IBM Industrie Europe où en tant qu'architecte il travaille sur des projets de type Industrie 4.0 dans le Manufacturing pour le secteur automobile, chimie pétrole, ferroviaire et aéronautique.

LinkedIn :

<https://fr.linkedin.com/in/serge-bonnaud-97b1527>

Twitter :

[@serge_bonnaud](https://twitter.com/serge_bonnaud)



Christophe Didier

Ingénieur diplômé de l'Epita et titulaire d'un MBA de Warwick Business School, Christophe Didier a travaillé dans les systèmes d'information militaires, les systèmes de santé des hôpitaux de Paris, l'aéronautique avec le programme A380, les villes intelligentes sur les projets Smarter Cities (Montpellier, Nice, Lille) et l'IoT (Internet of Things) en particulier pour les transports, la sécurité et l'énergie.

Il a été SME (Subject Matter Expert) pour les projets d'intégration complexe, porteur d'Offres et manager de pratiques de conseil en processus d'entreprise encadrant jusqu'à 40 personnes.

Après 20 ans dans le conseil en France et au UK, présent chez IBM depuis 2000, il a rejoint en 2014 les équipes techniques d'avant-vente en tant que Technical Director IoT, Mobile et Smarter Cities pour IBM France.

LinkedIn :

<https://www.linkedin.com/in/christophe-didier-bb9b425>

Twitter :

[@ChristofDidier](https://twitter.com/ChristofDidier)

Remerciements

Remerciements à Pascal De Vaucouleurs, Christophe Borde pour la qualité de leurs relectures approfondies et leur soutien tout au long de la rédaction de ce livre blanc.

Table des matières

03	Préambule
03	Définition : Qu'est-ce que la Blockchain
08	Pourquoi combiner Blockchain et IoT ?
11	IoT et Blockchain par secteur d'activité
12	Vision IBM de la Blockchain
12	Blockchain et IBM Cloud
14	Conclusion: IoT et Blockchain combinés
16	En savoir plus sur les technologies

Préambule

L'Internet des Objets (**IoT**) s'est récemment rapproché du sujet **Blockchain** et de nouveaux cas d'usage combinant les deux technologies apparaissent dans plusieurs industries ou domaines d'applications.

Avant de présenter la valeur **globale** de cette combinaison innovante, il est important de rappeler quelques définitions fondamentales sur l'IoT et Blockchain, tant le vocabulaire est spécifique et précis dans ces deux domaines.

La seconde partie de ce document décrira quelques cas d'usages pertinents dans le domaine industriel ainsi qu'un rappel sur l'ensemble des capacités IBM pour concevoir une solution mixant IoT et Blockchain.

Définition : Qu'est-ce que la Blockchain ?

Blockchain est un système qui gère les transactions s'opérant entre les partenaires d'un réseau distribué.

Lorsque l'on évoque la notion de transaction, il peut s'agir de transfert d'assets, de monnaies, d'échanges, d'écriture d'états dans un registre, ou de traçabilité à opérer sur des actions telles qu'achats, ventes, suivi ou déplacements d'objets, actes de fabrication ou de distribution.

Dès l'instant qu'un acte transactionnel entre plusieurs acteurs met en jeu des principes de véracité, de sécurité, de partage ou de traçabilité, alors l'étude et la mise en œuvre éventuelle d'un réseau Blockchain a du sens. ([Tweetez cette citation](#))

Le principe clé repose sur la notion de **confiance collective**, en opposition à la présence d'un tiers de confiance centralisé. En effet, dans un système Blockchain, il n'y a pas de tiers vérificateur ou d'organe central de contrôle tels que ceux que l'on rencontre dans les systèmes financiers

D'un point de vue technique, l'implémentation d'un système Blockchain s'appuie sur une séquence d'enregistrements chaînés et stockés dans une base de données distribuée intégrant un mécanisme innovant de réplication.

Une **Blockchain** préserve l'anonymat de ses utilisateurs en se basant sur des clés cryptographiques. De manière similaire, la signature des transactions et leur vérification utilisent la cryptographie asymétrique.

Le principe reste toujours le même : une clé privée permet de calculer une clé publique, mais l'inverse n'est pas possible. Ce principe déjà utilisé dans d'autres systèmes sécurisés est repris dans la Blockchain.

Enfin, le mécanisme de génération des paires de clés (clé privée et clé publique) nécessaire pour signer les transactions est fourni nativement par le cœur de la Blockchain.

Corrompre un groupe de nœud pour obtenir le consensus devient par conséquent difficile et coûteux. D'autre part, modifier un enregistrement n'impacterait pas la sécurité de la chaîne d'enregistrement global car il faudrait remonter à l'origine de la création du réseau pour reconstituer une transaction.

En dehors de la sécurité, deux autres concepts fondateurs sous-tendent la Blockchain, à savoir la notion de **Registre Distribué (Shared Ledger)** lié au **consensus** et la notion de **Contrat (Smart Contract)**.

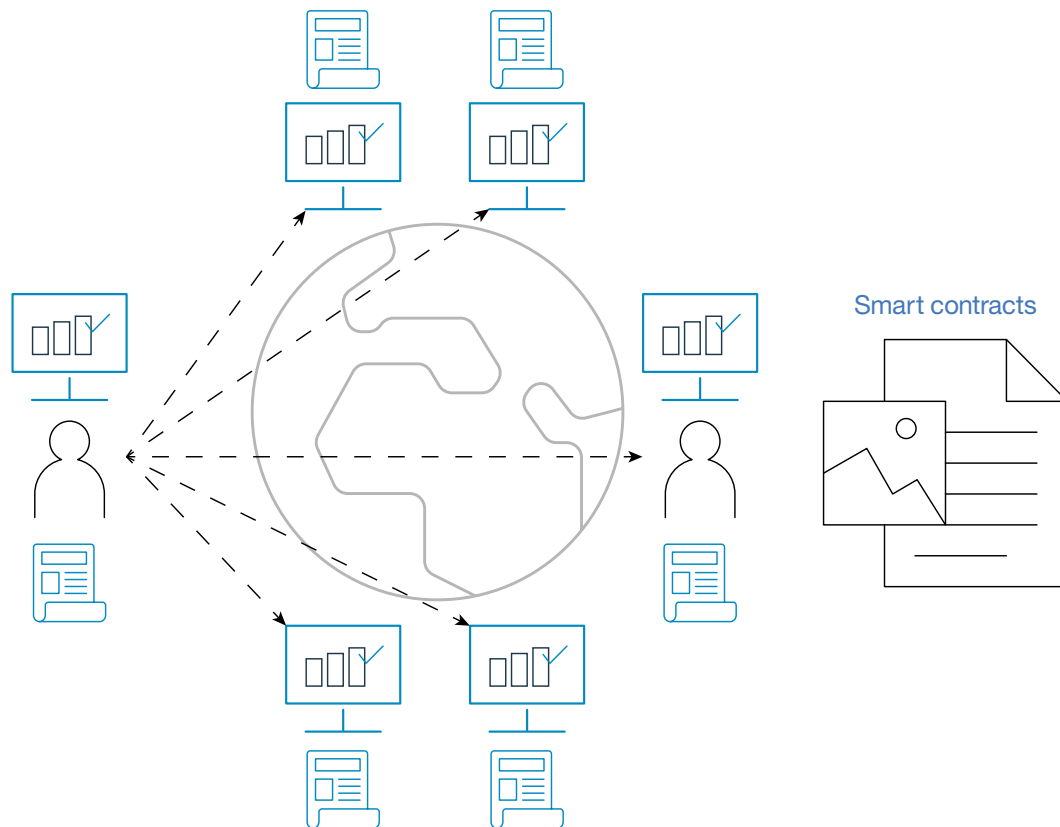


Figure 1:
Le monde de la Blockchain : Un réseau distribué

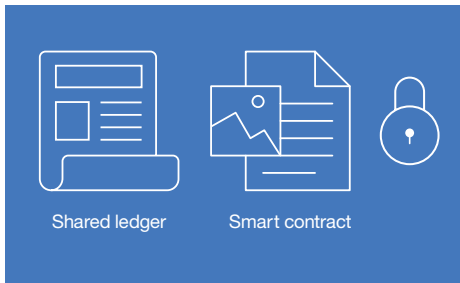


Figure 2:
Principes Blockchain



Figure 3:
Shared Ledger

Shared Ledger : Registre

Le registre répliqué et distribué est infalsifiable et contient tout l'historique des transactions sous la forme d'enregistrements individuels chaînés les uns aux autres et horodatés.

Un réseau de type **Blockchain** est donc un registre distribué et réparti offrant un haut niveau de sécurité, basé sur des algorithmes de cryptage très spécifiques, et contenant toutes les transactions effectuées depuis l'origine de la création du réseau. Il est partagé par tous les participants qui ont chacun une copie locale à travers le mécanisme de réplification.

Le réseau est géré par **droits** et **permissions**, de telle sorte que chaque participant ne voit que les transactions appropriées.

Dans les approches traditionnelles, un tel registre serait synchronisé par des API (Application Programming Interface) en mode point à point comme illustré par la figure 4 ci-dessous.

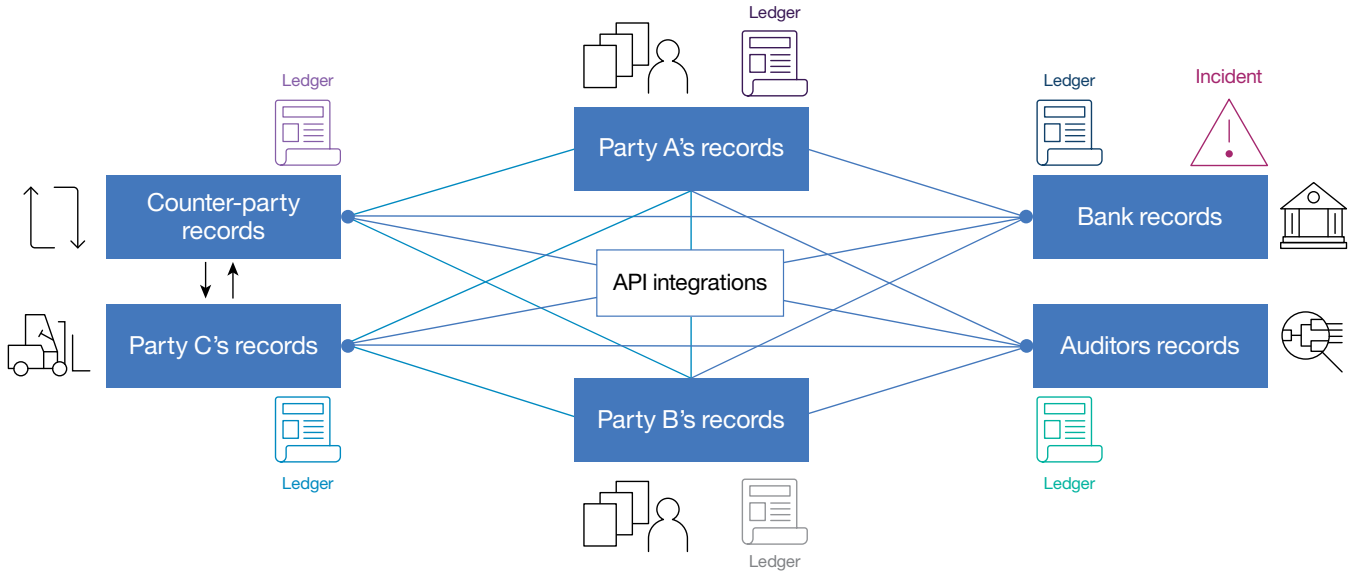


Figure 4:
Principes traditionnels de gestion d'un registre distribué

Cette approche pose des difficultés quand le nombre de points d'intégration augmente :

- la **vulnérabilité** globale s'accroît en termes de sécurité et l'un des nœuds peut souvent permettre de corrompre tout le réseau.
- la **supervision** globale de bout en bout devient difficile pour produire des états de suivi en temps-réel et anticiper au plus tôt les problèmes potentiels.
- les coûts de maintenance sont souvent **prohibitifs** pour assurer la diffusion d'informations à jour et pertinentes aux acteurs de la chaîne dans des temps raisonnables.

Dans une approche Blockchain, le registre est donc **distribué, synchronisé et dupliqué**, offrant ainsi la même vue **cohérente, à jour et sécurisée** à tous les participants du réseau. ([Tweetez cette citation](#))

Dans un réseau Blockchain, il existe un endroit unique pour déterminer la propriété d'un asset ou de la transaction : c'est le rôle du **registre distribué (Shared Ledger)**.

En effet, les participants partagent le même état du registre, mis à jour à chaque transaction à travers des mécanismes de réplication de type Peer To Peer.

En terme de sécurité, la cryptographie est utilisée pour s'assurer que chaque participant ne voit que les données pertinentes pour lui.

De plus, chaque participant a connaissance de l'origine de la transaction ou de l'asset ainsi que des éventuels changements de propriété de l'asset.

Enfin point essentiel dans la Blockchain, aucun participant ne peut signer ou modifier une transaction une fois qu'elle a été validée. Si une transaction génère une erreur, une nouvelle transaction doit être initiée et l'ensemble est visible par tous les participants.

Quant au contrat qui définit les conditions de la transaction ou du transfert de l'asset, il est embarqué dans la base de données répliquée.

Les participants du réseau se mettent d'accord sur les conditions de vérification de la transaction en appliquant chacun à leur niveau les règles du contrat.

Un mécanisme de consensus basé sur un calcul complexe visant à sélectionner les participants permet de valider la transaction et de démarrer l'acte de chaînage de l'enregistrement au réseau Blockchain (commit) : la réplication démarre, les registres sont mis à jour et la transaction est validée.

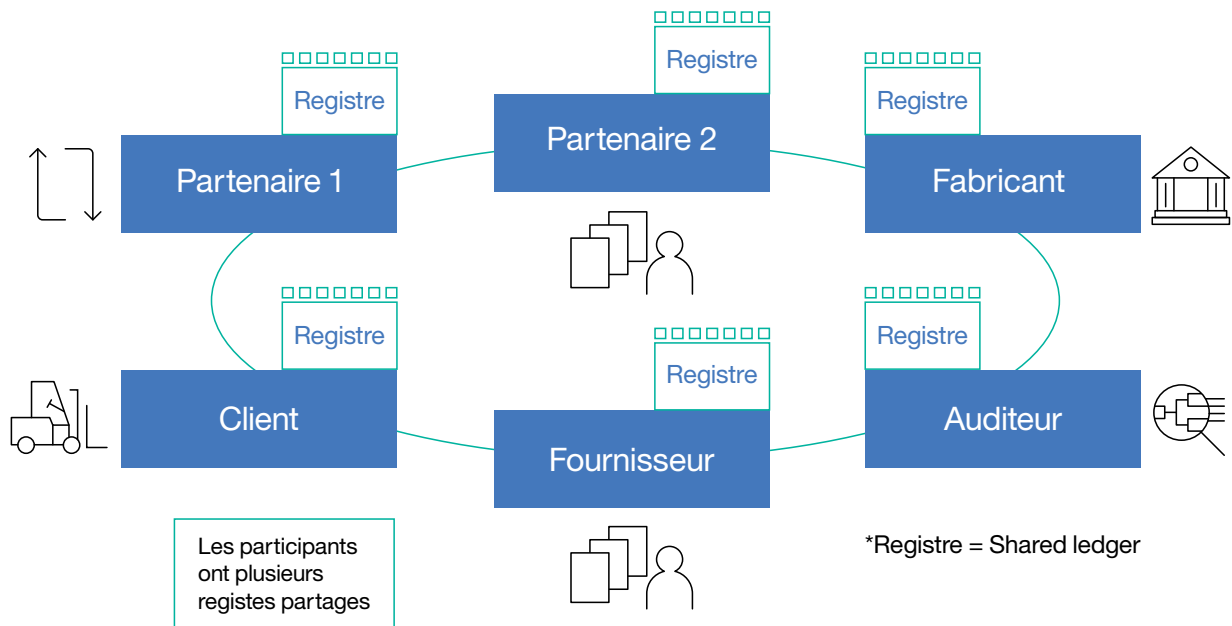


Figure 5: Gestion distribuée de registres partagés et répliqués dans Blockchain

Smart Contract : Contrat

Le contrat ou Smart Contract est le second concept fondateur après le registre.

Un contrat au sens Blockchain du terme contient les règles métier (Business Rules) qui définissent les conditions d'application à respecter et à vérifier pour une transaction où les conditions de transfert à appliquer pour un asset.

Le contrat contient aussi les règles qui définissent la propriété de l'**asset**, sa conformité, son état ou sa sécurité. Le contrat est **embarqué** dans la Blockchain et ses règles sont exécutées pendant la transaction par chaque participant au niveau applicatif. Il est vérifiable et on doit pouvoir le signer.

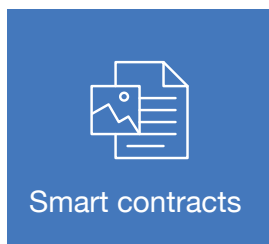


Figure 6:
Smart Contracts

Les contrats doivent être développés avec un langage de programmation approprié au niveau de chaque applicatif local connecté à la Blockchain.

D'un point de vue pratique, il est souvent nécessaire de modifier les applications clientes connectées au réseau Blockchain. Ces applications sont alors chargées d'implémenter et de vérifier la liste des règles rédigées dans le contrat.

De manière générale, un contrat peut embarquer tout type de règles ayant un sens applicatif et métier lors du transfert de l'asset ou lors de l'exécution de la transaction.

Définition : Qu'est ce que l'IoT ?

L'IoT, sujet mature depuis maintenant 4 ans, se transforme inexorablement pour passer d'un statut de technologie disruptive (vision de plate-forme de données et de services) à un statut d'**accélérateur** essentiel de la transformation digitale vécue par les entreprises.

Au-delà du fait que les objets et les produits deviennent de plus en plus bavards et génèrent un volume considérable d'informations, amenant le marché à offrir des plate-formes de collecte de données et de services basés sur l'Analytics, l'IoT a dorénavant un autre rôle stratégique à jouer. Posons-nous la question de savoir quel est ce nouveau rôle ?

Pour nous, l'IoT est clairement le moyen qui permet d'assurer la **continuité numérique (Digital Continuity)** tant attendue entre l'outil de production (**Manufacturing**), les études et l'ingénierie (**System Engineering & Software Development**) et la distribution (**Supply Chain**).

Afin d'assurer un lien fort entre le monde de la planification, des modèles et des prévisions et le monde physique de la fabrication, de l'ingénierie et de la distribution des produits ou services, il est nécessaire de mettre en œuvre deux concepts, à savoir le jumeau digital (**Digital Twin**) et le **Cyber Physical System (CPS)**.

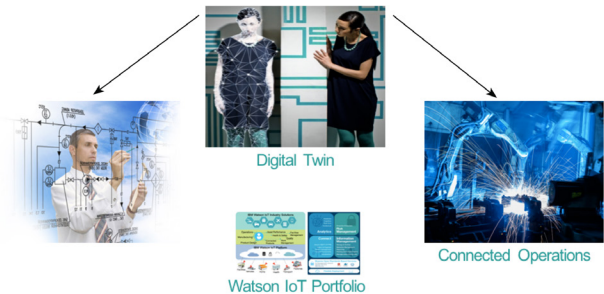


Figure 7:
Transaction IoT utilisant Blockchain

Pour implémenter les processus digitaux qui vont établir ce lien fort entre ces 3 mondes, historiquement non connectés, nous recommandons de mettre en œuvre une plate-forme de services telle que celle d'IBM : Watson IoT Connected Products (<https://www.ibm.com/internet-of-things/resources/connected-devices/>)

Cette plate-forme contribuera à établir la continuité numérique en permettant visibilité et partage d'une information à jour et cohérente.

Comme évoqué dans l'épisode 1 (IoT : Moteur de la transformation digitale), la plate-forme doit aller au-delà des fonctions traditionnelles telles que la collecte, l'analyse et la visualisation de données.

Elle pendra une dimension supplémentaire en intégrant le cognitif pour augmenter l'humain dans ses processus de décision, mais aussi la Blockchain pour ses concepts de registre et contrats, essentiels dans les processus manipulant des données issues des dispositifs IoT.

IoT Watson propose un service Blockchain basé sur la technologie Hyperledger améliorée et optimisée par les équipes de recherche et les laboratoires IBM.

Pourquoi combiner Blockchain et IoT ? (Tweetez cette citation)

Les capteurs qui équipent ou augmentent les produits physiques génèrent des données et des événements qui sont récupérés dans les processus par les partenaires au sein de leurs applications logicielles.

Nos objets, de plus en plus intelligents et connectés, embarquant de l'Analytics et du cognitif, sont en effet capables de collecter des données de l'environnement, de s'autodiagnostiquer, de générer de nouvelles informations sur eux-mêmes ou de réaliser des traitements analytiques complexes s'approchant de prises de décision autonomes dans le cas de la robotique. On parle alors de « Device Democracy ».

Certes, mais quelle confiance accorder à la « Device Democracy » ? Quelle confiance accorder à ces nouveaux processus issus de l'IoT où l'information est modifiée, partagée, utilisée, transformée et exposée en permanence ?

Comme expliqué en préambule, Blockchain est un système qui gère les transactions d'une manière innovante.

Ces dernières peuvent être financières comme avec le Bitcoin mais de toute autre nature également, comme par exemple la notification de déplacements de colis qui passent de zones en zones, l'information relative à l'obtention d'un diplôme ou d'un certificat, la prise en charge d'une assurance pour un business ou le partage d'informations clients entre partenaires.

La nature des transactions est de facto très variée. Si l'on poussait le trait à l'extrême, on pourrait affirmer que toute transaction pourrait être renseignée au sein d'un système Blockchain.

Techniquement cela reste vrai, mais logiquement il faut y trouver un intérêt et une valeur mesurable, que cela soit d'un point de vue business, légal, sociétal ou autre.

Cas d'usage #1 : Blockchain et Transport Maritime

Tout d'abord il est important de rappeler que la Supply Chain maritime souffre de maux bien connus de longue date :

- Manque de visibilité parmi tous les acteurs.
- Manque d'anticipation et difficulté à gérer les crises.
- Trop d'activités manuelles et utilisant du papier.
- Nombreuses erreurs et des retards dans les approvisionnements.

Dans cet exemple mis en œuvre chez Maersk, un transporteur par containers souhaite commercialiser un service qui nécessite une assurance supplémentaire sur l'ensemble du trajet.

Le container instrumenté surveille via des capteurs les conditions de transport (vibration, température, humidité, magnétisme, position ...).

Ces informations sont remontées dans la Blockchain afin de déclencher des paiements partiels lors de l'acheminement ainsi que des pénalités (en lien avec l'assureur) si les conditions du contrat ne sont pas respectées (trop chaud, trop humide, trop malmené ...)

IBM et le transporteur maritime Maersk ont annoncé développer une solution commune basée sur un réseau Blockchain (Tweetez cette citation)



Figure 8:
Maersk et IBM développe un réseau Blockchain

En sélectionnant Blockchain et IBM en tant que partenaire, Maersk améliore la visibilité et la traçabilité de ses processus de Supply Chain. <http://www-03.ibm.com/press/us/en/pressrelease/51712.wss>

Des applications selon le même principe sont possibles pour le suivi, la traçabilité et la maintenance des pièces détachées dans l'aviation, l'automobile (partage du carnet d'entretien du véhicule) et la construction des bâtiments (carnet de certification)

Cas d'usage #2 : Blockchain et Maintenance dans l'aéronautique

Blockchain permet de renforcer les moyens de lutte contre la contrefaçon, de réduire les coûts opérationnels de maintenance et d'améliorer la qualité de service globale en assurant le partage d'informations vérifiées et sécurisées durant tout le cycle de vie d'un équipement, d'une pièce détachée ou d'un device.

Prenons un exemple précis ... L'information « Remplacement d'une pièce lors d'une activité de maintenance non-prévue sur un avion en service entre deux décollages » est un événement temporel important et critique que l'on peut enregistrer dans la Blockchain.

Les questions importantes à se poser sont les suivantes :

- Qui a remplacé la pièce ?
- Qui a demandé le remplacement ?
- Quelles étaient les certifications de la personne concernée?
- Sur quel appareil ?
- Quand a-t-elle été remplacée ?
- Quelle configuration a été appliquée ?
- Quel test a été fait pour s'assurer du bon fonctionnement global de l'appareil ?

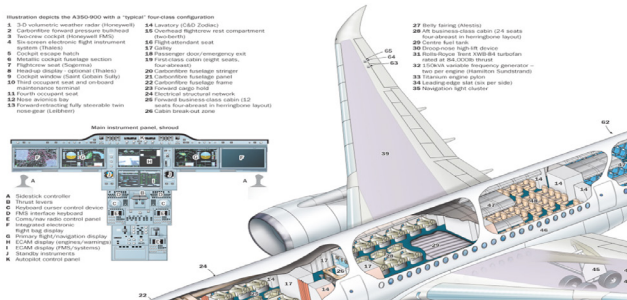


Figure 9: Blockchain dans la maintenance aéronautique

Dans le cas de cette activité de maintenance non planifiée, Blockchain :

- Apporte de la **transparence** pour toutes les parties-prenantes qui ont besoin d'être informées de ce changement, à savoir le Flight Dispatcher, les opérations aériennes, les équipages, la compagnie aérienne, l'exploitant et les services de maintenance. Ce partage est réalisé grâce à l'utilisation d'un journal centralisé et sécurisé : Shared Ledger.
- Améliore la **performance** globale en facilitant la coopération sécurisée entre partenaires de la compagnie aérienne via les « Smart Contract ». Le contrat porte dans cet exemple sur les règles à vérifier avant de lancer l'inspection de l'avion et les règles à vérifier pour enregistrer l'activité de remplacement de la pièce.

- Augmente la **confiance** lors des transactions en se basant sur un mécanisme de « consensus distribué » sans nécessité d'utiliser une tierce partie. Dans le cas mentionné, le mainteneur, le contrôle aérien, les opérations aériennes et le pilote confirment le remplacement de la pièce.

En conclusion, Blockchain dans ce cas d'usage :

- permet de **mentionner** et **tracer** la provenance de chaque pièce de manière précise et non falsifiable
- rend l'information **accessible** à chaque fabricant, propriétaire de flotte, mainteneurs et autorités de régulation.
- génère l'**historique** complet des interventions et des configurations modifiées sur les avions par tâches de maintenance (figure ci-dessous n°10)

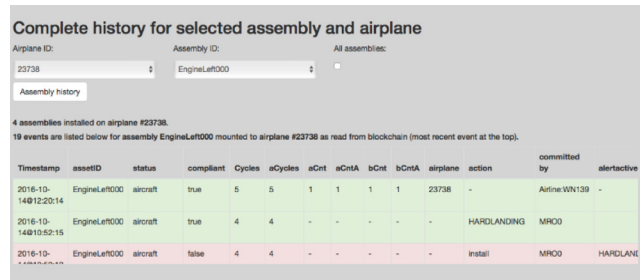


Figure 10: Historique sous Blockchain des interventions sur un avion en maintenance

Cas d'usage #3 : Blockchain et Logistique dans l'industrie du bois

Kouvola, une ville Finlandaise connue pour son industrie de bois, constitue le centre logistique ferroviaire le plus important de Finlande.

Plus de 500 entreprises de logistique assurent l'ensemble des activités de cette industrie. Cette ville veut, à l'aide de la Blockchain, améliorer la gestion de son activité, simplifier les processus logistiques de transport, optimiser les liens entre les différents acteurs de la chaîne de valeur. <https://www-03.ibm.com/press/us/en/pressrelease/49029.wss>

La démonstration interactive (lien à cliquer ci-dessous) du

suivi d'un conteneur et de son contenu au fur et à mesure de ses déplacements d'un bout à l'autre de la chaîne logistique, via de nombreux transporteurs montre que la Blockchain peut garantir la traçabilité des événements liés à la chaîne du froid tout au long du trajet d'un conteneur.

La démonstration interactive (lien ci-dessous) illustre comment la Blockchain garantit la traçabilité des événements liés à la chaîne du froid tout au long du trajet d'un conteneur.
Démonstration interactive: <https://discover-iot-blockchain.eu-gb.mybluemix.net/iot-blockchain.html>

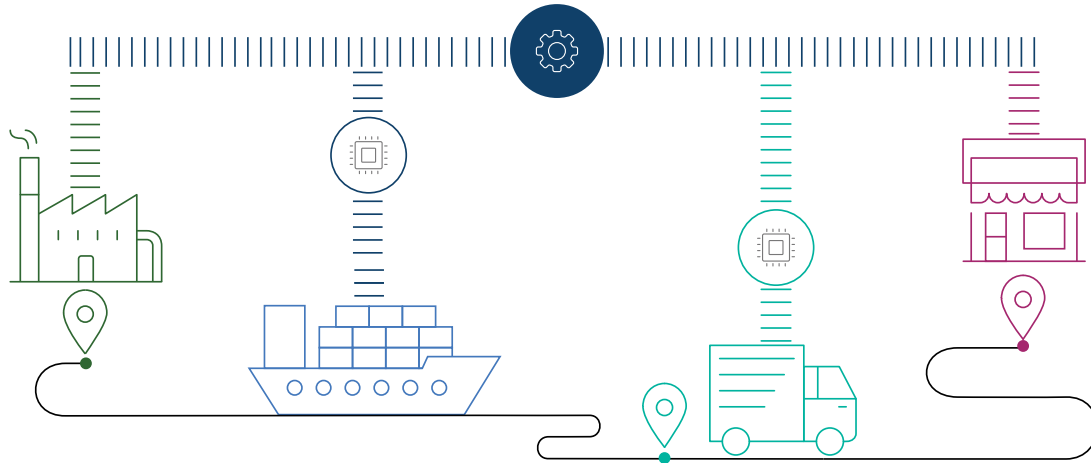


Figure 11: IoT & Blockchain

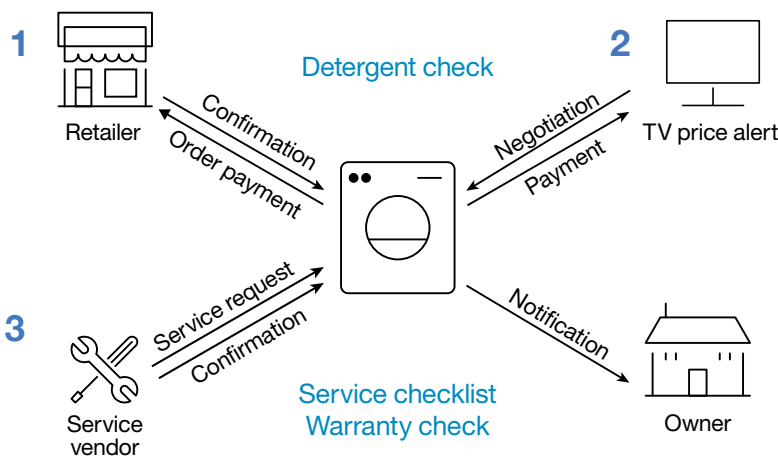
En lisant ces 3 cas d'usage, on perçoit aisément que des activités manipulant des données sensibles entre plusieurs partenaires peuvent donc être exécutées en transparence et en toute confiance via l'enregistrement d'événements au sein d'un journal répliqué (non-centralisé) et non-modifiable.

Mais quel est donc le rapport avec l'IoT ? Regardons comment l'IoT entre en scène en apportant de l'eau au moulin de la Blockchain.

En 2015, IBM avec son projet de recherche ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) a créé le concept de « Device Democracy », qui vise à développer un réseau d'appareils connectés reposant sur la Blockchain.

Le but était de permettre à des entités distribuées (des devices : une machine à laver, une télévision ...) d'effectuer des transactions avec des partenaires : commandes de consommables (liquide de lavage), notification de niveaux (énergie, liquides, ...), demandes de prix.

Tout cet écosystème, étant en « démocratie » totale, ne s'exécute pas via des systèmes centraux mais bel et bien directement entre « devices citoyens », en autonomie et de manière sûre et transparente.



Use case scenarios

- 1 Consumables marketplace
- 2 Service marketplace
- 3 Energy marketplace

Figure 12: ADEPT : 1er démonstrateur IoT & Blockchain (2015)

IoT et Blockchain par secteur d'activité

Les cas d'utilisation IoT utilisant le Blockchain se sont depuis multipliés dans tous les secteurs industriels :

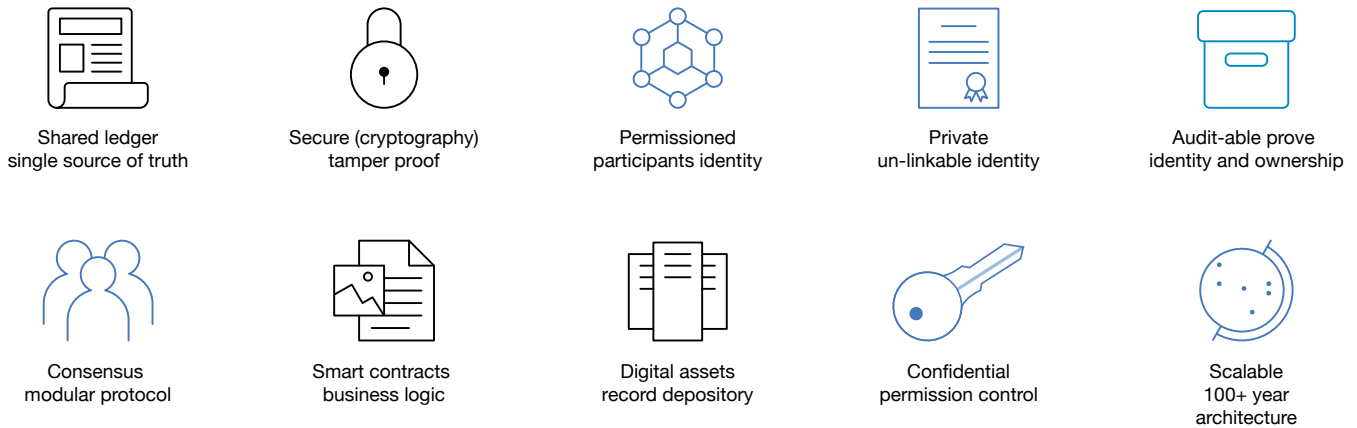
Secteur	Cas d'utilisation	Données partagées	Partenaires
Transport	Suivi d'envoi logistique Partage des documents de transports	Localisation Conditions de transports (température, humidité ...) Documents (douanes, bon de chargement)	Expéditeur, transporteur destinataire, douanes, banque
Maintenance	Traçabilité des pièces détachées durant leur cycle de vie	Identification des pièces Information sur l'usage Information sur la maintenance	Constructeur de pièces détachées, constructeur de produits à base d'assemblages, organisme de réparation, propriétaire, agence de régulation
Logistique	Partage de l'offre et de la demande Visibilité sur les localisations et l'état de réalisation des pièces détachées	Gestion de la demande Volumes produits Provenance des pièces (ID, date d'expiration, etc. ...)	Fournisseur, constructeur, ...
Organisme de Régulation	Partage de document avec un organisme public	Document de conformité Information d'utilisation et de maintenance	Organisme public, opérateurs et constructeurs
Gestion de bâtiments	Enregistrement des accès et utilisations d'un bâtiment	Enregistrement du fonctionnement des équipements (Clim, Chauffage, Air, Lumières, Alarmes ...) Enregistrement des accès individus	Propriétaire de bâtiments, gestionnaire d'immeubles ...
Energie	Traçabilité de l'impact Carbone	Crédit Carbone Production Carbone	Gestionnaire Carbone, citoyens...
Télécommunication	Smart Building	Evénements réseaux au sein d'un bâtiment	Fournisseur de passerelles et routeurs réseaux
Automobile	Acheminement vers distributeurs	Etat des véhicules Localisations des véhicules durant la distribution	Constructeurs, distributeur, assurance, acquéreur ...
Aéronautique	Cycle de vie des pièces	Utilisation des pièces Maintenance des pièces	Constructeurs, Partenaire maintenance, compagnies aériennes
Banque	Vente aux détails	Monitoring des ventes aux détails Intégration des crédits	Banques, commerçants

Vision IBM de la Blockchain

Un peu d'histoire récente

Le code IBM fut développé à travers une collaboration de plus de 35 chercheurs et développeurs dédiés à la fondation Linux. Plus de 100 spécialistes techniques ont rendu le projet de recherche concret et délivré la solution actuelle.

IBM a ensuite décidé d'offrir le code de son projet Blockchain à la communauté Open Source Hyperledger.



Black: standard properties of Blockchain
Blue: added properties/uniqueness of IBM

Figure 13:
Les améliorations IBM à Hyperledger

Afin d'assurer la pérennité et l'ouverture de sa solution Blockchain, IBM participe activement et fortement au projet open source Hyperledger en y apportant les volets industrialisation, sécurité et identification des participants aux transactions (pas de mode anonymous) ainsi que la possibilité de choisir son algorithme de consensus ajoutée à une gestion des Certificate Authority plus exigeante.



Figure 14:
Project open source Hyperledger (<https://www.hyperledger.org>)

Blockchain et IBM Cloud

Les services Blockchain sont disponibles chez IBM en particulier sur IBM Cloud et en combinaison avec la plateforme Watson IoT.

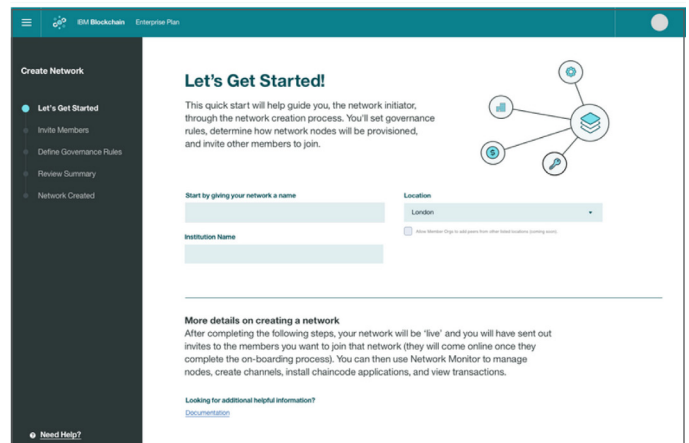


Figure 15:
Démarrer avec Blockchain sous IBM Cloud

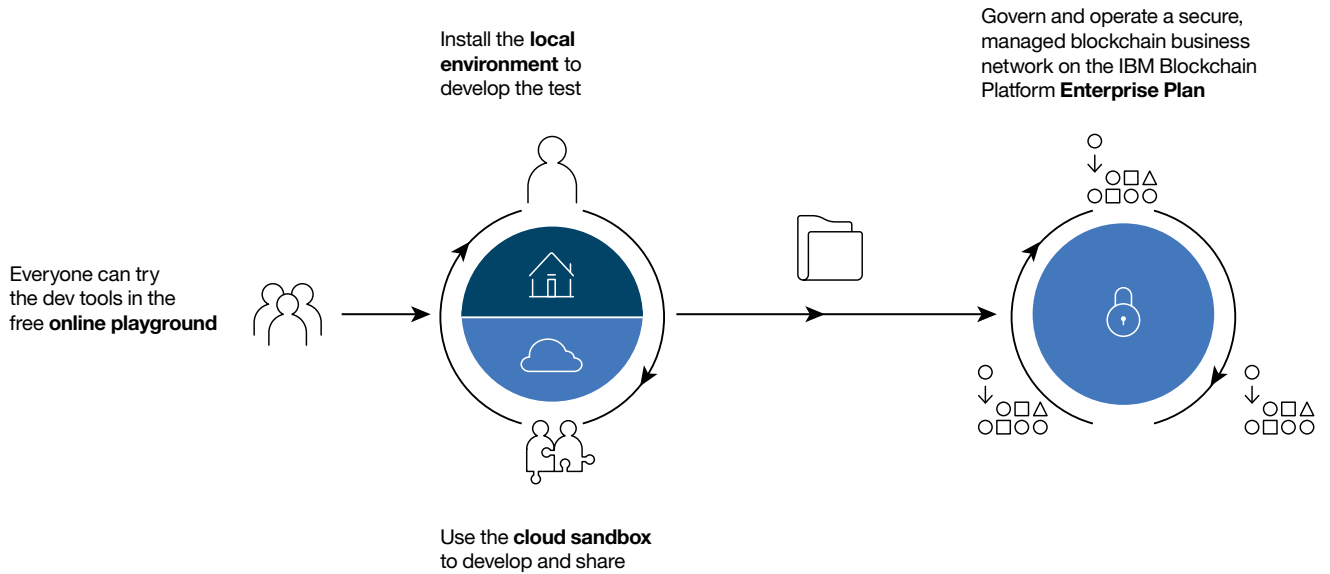


Figure 16:
Blockchain et IBM Cloud pour les développeurs

Ces services font partie intégrante de la section « Risk Management » de la solution IBM Watson IoT.

A ce titre, ils sécurisent les transactions en utilisant les capacités non-modifiables, transparentes, distribuées du journal Blockchain durant les remontées événementielles des données en provenance des objets (devices).

Le service Blockchain au sein de la plate-forme IBM Watson IoT

Cette section explique comment se déclenche concrètement une transaction IoT dans un contexte blockchain en prenant comme exemple la plate-forme d'IBM Watson IoT.

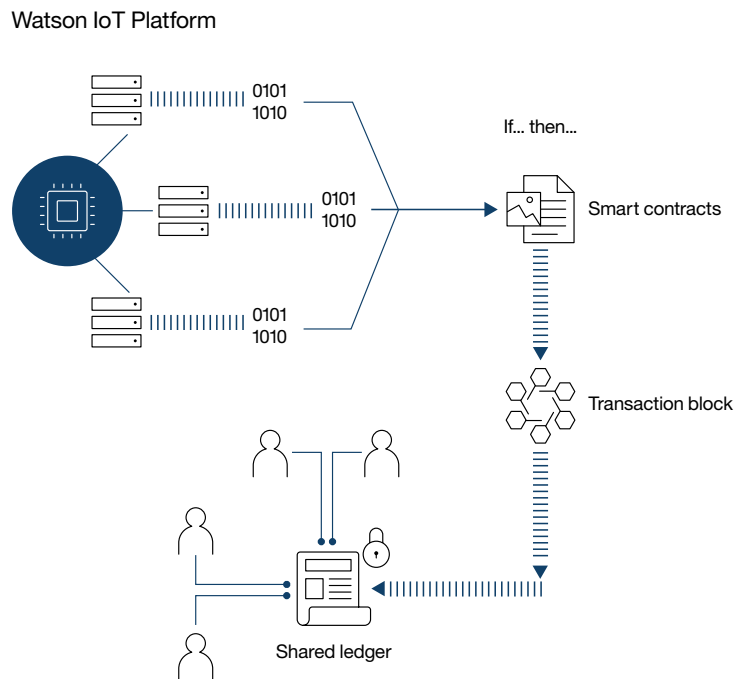


Figure 17:
IBM Blockchain et Watson IoT

De manière très pragmatique et détaillée sur le schéma ci-dessous, une transaction IoT peut être déclenchée par un Device, via un envoi de message suivant le protocole MQTT, de manière sécurisée vers la plateforme Cloud Watson IoT.

Grâce à l'intégration Blockchain au sein de la plateforme IoT (Proxy), cet événement déclenche à son tour son enregistrement dans le réseau des partenaires du Blockchain concerné.

Bluemix (Hosted)

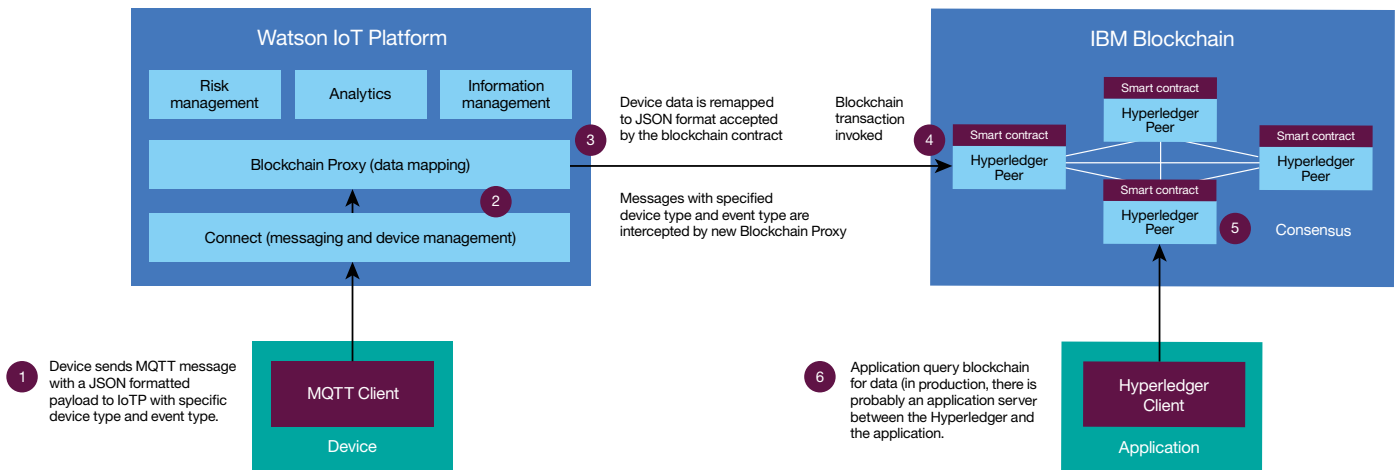


Figure 18: IBM Blockchain et Watson IoT

Ces concepts imaginés et prototypés dès 2015 sont d'ores et déjà disponibles et expérimentés chez des clients partout dans le monde et en France, comme par exemple au Crédit Mutuel Arkéa : (<https://www.youtube.com/watch?v=AI0TbawHqR4>)



Figure 19: Référence IBM France sur Blockchain

Un Smart Contract peut être appliqué de manière automatique si certains critères sont réunis (atteinte d'un niveau donné de transaction par exemple, arrivée sur une zone, dépassement d'une durée ...).

Cet automatisme permettra ensuite de renseigner d'autres informations qui seront alors utilisées en temps-réel par la ou les applications finales.

Conclusion : IoT et Blockchain combinés

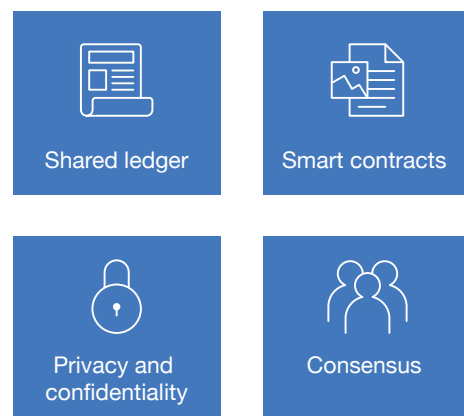


Figure 20: Rappel — Les 4 principes de la Blockchain

Comme le souhaitait IBM dès le projet ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) en 2015, nous prônons :

Un IoT plus fiable et sécurisé

- IBM a très tôt proposé un fonctionnement décentralisé de la Blockchain reposant sur un principe Peer To Peer afin d'améliorer la sécurité globale de la chaîne. En effet, contrairement aux réseaux centralisés, un réseau en peer-to-peer ne dépend pas d'un acteur unique, mais de multiples nœuds composés par les utilisateurs du réseau. Ainsi, plus il y a d'utilisateurs, plus le réseau sera résistant aux attaques.
- Incorporer la Blockchain à l'IoT nécessite de penser la confidentialité de manière différente : la propagation de données personnelles devra être réalisée par le propriétaire du device. De même, le possesseur de l'objet aura la charge de définir les règles de collaboration de l'objet avec son environnement.

Des objets connectés mieux valorisés

- Il est important d'avoir une identité unique pour chaque objet connecté à la Blockchain. En connectant un objet à la Blockchain, un concepteur permet à ce dernier de transmettre des données sur la Blockchain pendant tout le cycle de vie.
- De cette manière, la Blockchain devient une sorte de référentiel produit à haute fiabilité.

Une capacité d'interaction renforcée.

- Un objet connecté **échange** par nature avec son environnement et peut ainsi engager des transactions de son propre chef avec d'autres objets lors d'un processus décisionnel basé sur un algorithme analytique.
- Cela implique que ce dernier soit capable de **reconnaître** les autres participants du réseau et de calculer un niveau de confiance afin d'initier la transaction. Or c'est exactement ce que permet la Blockchain.

A titre d'exemple, IBM a imaginé une machine à laver capable de passer des commandes de détergents de manière automatique auprès du fournisseur.

Pour cela, il est nécessaire d'écrire un **contrat** entre le constructeur de la machine et son fournisseur, puis que la machine à laver soit capable de s'auto-diagnostiquer et de mesurer son état, de choisir un fournisseur approprié, de générer la demande et attendre la réponse du fournisseur.

Quel futur pour le couple IoT et Blockchain ?

Les objets connectés deviennent de plus en plus autonomes en **intégrant** du cognitif et sont capables de prendre des décisions en contexte en se basant sur la collecte de données en temps-réel.

Les utilisateurs des objets connectés vont donc devoir élaborer des **Smart Contracts** qui listeront les règles métier prévoyant les différents scénarios possibles d'interactions entre les participants du réseau.

Quant au registre partagé (Shared Ledger), il servira à enregistrer les actions réalisées par les objets (échanges de flux, interactions ..) et les rendra ainsi visibles à tous les participants du réseau.

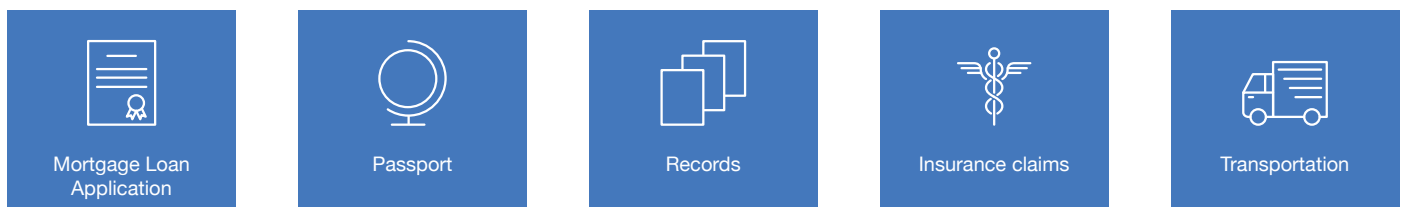


Figure 21:
Blockchain et les industries : Une infinité de cas d'usage

En conclusion, l'intégration entre l'IoT et la Blockchain, bien loin de Bitcoin et du monde financier, semble être le mariage parfait pour faciliter de manière hautement sécurisée les activités collaboratives (Sales, Manufacturing, Supply Chain) entre plusieurs partenaires d'un écosystème ouvert.

En savoir plus sur les technologies

Blockchain

- IBM Blockchain: <https://www.ibm.com/blockchain>
- IBM Blockchain : Offres : <https://www.ibm.com/blockchain/offerings.html>
- Watson IoT et Blockchain : <https://www.ibm.com/internet-of-things/fr-fr/iot-solutions/watson-iot-platform/>

IoT

- L'Internet des Objets, vecteur de la transformation : <https://www.ibm.com/internet-of-things/fr-fr/digital-transformation/>

© Copyright IBM Corporation 2017

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
December 2017

IBM, the IBM logo, ibm.com, and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/us/en/copytrade.shtml>

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The information in this document is provided "as is" without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. **IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.**

