Blockchain

La nouvelle révolution technologique ?

Comment cette nouvelle technologie pourrait fondamentalement changer nos relations aux autres ainsi que notre façon de vivre et de travailler.

capteo

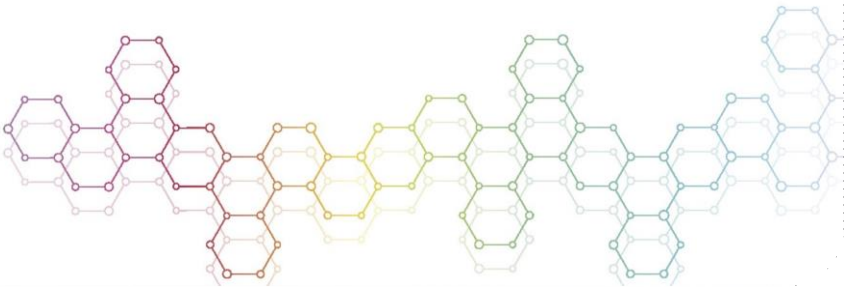
STRATEGY & MANAGEMENT CONSULTING

Juin 2018

capteo

Introduction à la Blockchain

01



Dans son dernier rapport, le Forum Economique Mondial (WEF) avertit qu'une nouvelle révolution industrielle est en marche. Cette « Industrie 4.0 » englobe la transformation des moyens de production, de management et de gouvernance.

Après une première révolution (mécanisation de la production grâce à l'eau et la vapeur), une deuxième (production de masse grâce à l'énergie électrique) et une troisième (automatisation de la production grâce à l'électronique et aux technologies de l'information), nous entrons désormais dans une nouvelle ère : celle de la **révolution numérique** via l'adoption de technologies émergentes.

La combinaison de ces technologies, dites de « rupture », va changer radicalement nos rapports aux autres, notre manière de vivre, de travailler… Cela va impacter tous les secteurs d'activité, partout dans le monde, à un rythme beaucoup plus important que par le passé.

Parmi ces technologies figure la **Blockchain ou technologie des registres distribués (Distributed Ledger Technology)**.

Lorsqu'un certain Satoshi Nakamoto publie en 2008 un article [(1)] qui présente cette nouvelle technologie, il la pense comme une alternative à nos systèmes de confiance traditionnels, basée uniquement sur un réseau distribué P2P (en anglais 'peer-to-peer') et s'appuyant sur un protocole informatique de cryptographie asymétrique.

Satoshi Nakamoto (dont l'identité reste encore contestée à ce jour) la décrit comme un moyen de conserver de l'information de façon extrêmement sécurisée mais surtout il y intègre une dimension sociale incitant chaque nœud (c'est-à-dire chaque machine) à collaborer avec l'ensemble du réseau pour garantir la fiabilité des informations.

Chaque nouvelle entrée au sein du réseau est distribuée à tous les nœuds du réseau qui vont ensuite l'évaluer. Si elle est contestée, le système arbitre en faveur d'un consensus adopté par plus de la majorité des nœuds. Sinon, elle est enregistrée dans un conteneur numérique, un bloc, de façon permanente, sans modification ni suppression possible. On obtient ainsi **une chaîne de blocs chronologiquement liés entre eux, capables de s'organiser pour éliminer ou supprimer toute information incorrecte ou falsifiée** : la Blockchain est née !

Au départ, la volonté de cet inventeur japonais était de créer une monnaie numérique alternative, le Bitcoin, s'appuyant sur ce protocole de Blockchain sécurisé, permettant ainsi l'origination d'un système de confiance alternatif au système bancaire pour émettre et recevoir des paiements. Mais il entrevoit déjà un potentiel beaucoup plus large de sa technologie : sa capacité à remettre en cause toute une partie de nos organisations existantes, en transférant la fonction de confiance à son système de façon totalement transparente et distribuée, en opposition aux systèmes verticaux, centralisés autour d'agents de contrôles : les banques, les notaires, les dépositaires centraux, les états…

Confinée à un cercle d'experts dans un premier temps, la technologie Blockchain prend son essor à partir de 2015 et déclenche une vague d'intérêt de plus en plus forte de la part des entreprises, des institutions mais également du grand public. Intérêt parfois irrationnel si l'on pense à cette entreprise de thé qui a augmenté son cours en bourse de 286% uniquement en accolant le terme Blockchain à son nom [(2)].

1) http://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/#selection-33.98-33.223
2) https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-Blockchain

Plus qu'un phénomène de mode numérique, une définition encore mystérieuse et naissante sur les réelles possibilités d'industrialisation, la **Blockchain présente les caractéristiques d'une technologie disruptive majeure induisant une véritable révolution technologique dans les échanges transactionnels** : elle rend obsolète tout un ensemble d'acteurs de l'écosystème, réduisant les coûts et les contraintes tout en augmentant la fiabilité générale du système à l'aide de principes techniques que nous détaillerons au travers de cette publication.

Au-delà d'être une technologie de transmission et de stockage numérique totalement décentralisée et sécurisée, contenant la liste de tous les échanges ou transactions effectuées entre les utilisateurs, la Blockchain a évolué rapidement pour offrir des innovations supplémentaires. En particulier les 'smart contracts', ouvrant ainsi la voie à divers cas d'usage et de règles de gestion modulables, pouvant ainsi s'adapter aux besoins fonctionnels des entreprises publiques ou privés.

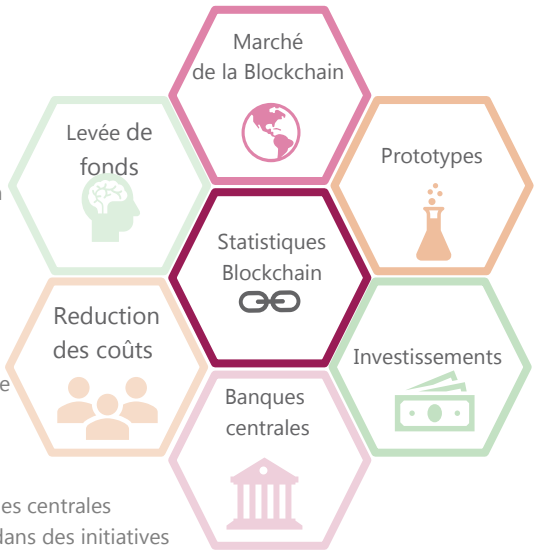
Le phénomène ne cesse de croître et de s'amplifier, avec de nombreuses initiatives expérimentales en cours au sein des secteurs bancaires, financiers et assurantiels, et déjà les premiers résultats concrets à l'échelle opérationnelle.

Il reste à imaginer ce que la maturité de la Blockchain pourrait apporter au sein des marchés, des entreprises et de notre quotidien. Quelles sont en l'état les limites et les contraintes de cette technologie et comment celles-ci pourraient-t-elles évoluer ? Quelles stratégies business à envisager autour de ce phénomène ? Quels sont les impacts organisationnels à prévoir ? Quelles pourraient être les différentes applications pertinentes à mettre en œuvre au sein du secteur financier ? Enfin, si cette technologie était amenée à redéfinir la fonction de contrôle, sur quelle base juridique le ferait-t-elle ?

Beaucoup de questions en effet se posent !

Nous avons donc souhaité vous apporter notre propre éclairage sur la Blockchain et vous permettre d'en appréhender les concepts-clés de manière simple et rapide. Comprendre ainsi plus précisément de quoi on parle, son mode de fonctionnement et les différents éléments structurants de cette technologie. Balayer les différents cas d'usage, les contraintes qui persistent, les impacts organisationnels à prévoir ou encore le cadre juridique et réglementaire qui se pose face à cette technologie, et ses limites.

24 Milliards $, estimation du marché de la Blockchain d'ici 2024



5,6 Milliards$ de levée de fonds en 2017 via émission de crypto-monnaie (ICO)

90% des principales banques américaines et européennes ont lancé des prototypes basés sur la Blockchain

8 à 12 Milliards$ par an de réduction des coûts pour le secteur bancaire grâce à cette technologie

1.4 Milliards $, montants des investissements sur la technologie en 2016

+90 banques centrales engagées dans des initiatives Blockchain

Source: www3.weforum.org
https://expandedramblings.com/index.php/blockchain-statistics/

Présentation de la Blockchain

02

La **Blockchain est fondamentalement une technologie de stockage et de transmission d'informations sécurisée**, à l'image d'une base de données distribuée, en y intégrant en plus une protection cryptographique des données et en permettant la conservation de l'historique de tous les échanges effectués entre ses participants.

Echange de valeur, transfert de propriété, ou encore notarisation… ces transactions se réalisent grâce à une chaîne de blocs contenant les données, d'où le terme 'block' - 'chain'.

Mais à la différence d'une base de données classique, la Blockchain introduit un nouveau type de gouvernance décentralisée, intégrée et gérée par la technologie, sans intermédiaire qui ne requiert pas la présence d'une tierce autorité de contrôle.

En remettant en cause l'utilité des acteurs de confiance traditionnels (notaires, banques, chambres de compensation…), elle permet d'envisager une approche totalement nouvelle et disruptive de nos organisations.

En résumé, la technologie Blockchain repose sur trois grands principes techniques fondamentaux :

1. **Une architecture décentralisée** ou architecture pair à pair pour assurer la résilience du système.
2. L'utilisation de **cryptographie** asymétrique pour garantir la sécurité des informations.
3. La mise en place d'un algorithme, appelé **consensus**, pour éliminer le risque de fraude et garantir la confiance au sein du système.

L'ARCHITECTURE DÉCENTRALISÉE OU ARCHITECTURE PAIR À PAIR (P2P)

On parle d'architecture centralisée lorsqu'une machine ou nœud fait office d'organe central, c'est le modèle client-serveur.

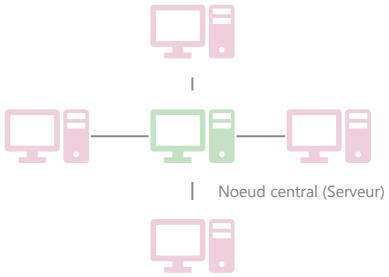


Illustration : Architecture centralisée

Une architecture ou un réseau informatique est dit distribué dès lors que toutes les ressources ou informations du réseau ne sont pas centralisées sur une même machine.

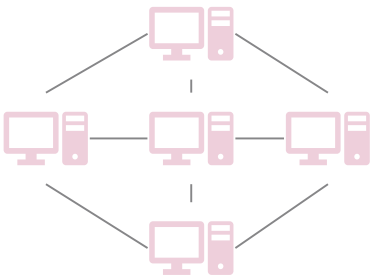


Illustration : Architecture décentralisée

En l'absence d'organe central dans une architecture distribuée, les informations sont distribuées sur tout ou partie du réseau. Si un nœud du réseau devient inactif suite à une attaque, l'information restera disponible auprès des autres nœuds : ces architectures sont donc des références en termes de robustesse et de résilience Internet est, par exemple, construit sur une architecture distribuée.

LA CRYPTOGRAPHIE ASYMÉTRIQUE

C'est une méthode de cryptage apparue en 1976 grâce aux travaux des chercheurs américains Whitfield Diffie and Martin Hellman.

Elle se base sur l'utilisation de deux clés, l'une publique utilisée pour chiffrer les informations et l'autre dite 'privée', uniquement connue de son propriétaire et nécessaire au déchiffrement. Cette méthode permet de :

- Chiffrer le message sans devoir transmettre la clé de déchiffrement : l'expéditeur utilise la clé publique du destinataire pour coder son message. Le destinataire utilise sa clé privée pour décoder le message de l'expéditeur, garantissant la confidentialité du contenu.
- Garantir l'identité de l'expéditeur : l'expéditeur utilise sa clé privée pour coder un message que le destinataire peut décoder avec la clé publique de l'expéditeur.

LE MÉCANISME DE CONSENSUS

Le **consensus** désigne le mécanisme de gouvernance qui permet à une architecture Blockchain de valider la validité d'une information. La Blockchain étant basée sur une architecture décentralisée, il n'existe pas de nœud central ayant vocation à servir d'organe de contrôle pour vérifier et valider les informations stockées au sein du réseau.

Cette étape de vérification est au contraire distribuée sur l'ensemble des nœuds, l'objectif étant de faire émerger une validation globale au sein du réseau, un consensus. Chacun de ces nœuds vérifie la validité de la nouvelle transaction en calculant divers algorithmes, on dit dans ce cas qu'ils minent la nouvelle transaction, les nœuds en charge du calcul étant les mineurs.

Lorsqu'un mineur a validé une transaction, il l'insère dans un bloc et rajoute chronologiquement ce bloc à la liste des blocs existants : la transaction est enregistrée dans la Blockchain. Les blocs sont donc liés aux uns et aux autres de telle sorte que si on souhaite modifier un bloc, on est contraint de modifier toute la chaine.

Le point crucial de ce mécanisme est le fait que le minage repose sur la résolution de problèmes mathématiques complexes : c'est un processus complexe qui nécessite un certain délai de calcul

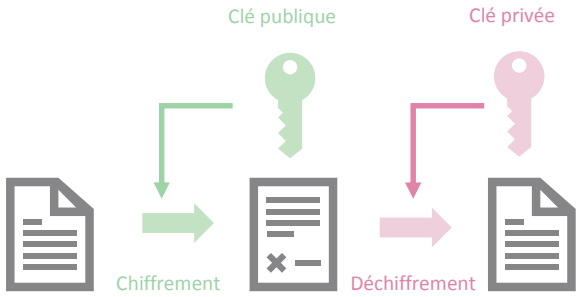


Illustration : Méthode de cryptage

Note : En pratique, on distingue différents types de consensus selon les Blockchains considérées : Proof Of Work, Proof Of Stake… De même que pour des raisons d'efficacité, certaines Blockchains limitent les activités de minage sur certains nœuds qui font uniquement office de validateurs pour le compte de nœuds restants.

Ainsi dans l'hypothèse où un nœud frauduleux souhaiterait insérer une fausse transaction, encore faudrait-il qu'il ait autant de puissance de calcul que la moitié du réseau réunie pour « battre » les nœuds sains qui continueront de travailler sur les transactions valides et remettre ainsi en cause le consensus établi au sein du réseau.

La puissance de calcul et les coûts d'énergie nécessaires à la réalisation de cette fraude supprimeraient toute perspective de gain. Notons au passage que les ressources (puissance de calcul, énergie, stockage) nécessaires au fonctionnement de la plate-forme ne sont pas pilotées et distribuées par une autorité centrale. Elles sont fournies par les nœuds eux-mêmes.

Pour compenser cet investissement mais également inciter les nœuds à le poursuivre, la Blockchain crée des jetons numériques, des **Token**, sorte de monnaie virtuelle qu'elle distribue aux nœuds ou mineurs ayant calculé toute nouvelle transaction.

De facto, puisque l'infrastructure est distribuée sur l'ensemble des points du réseau, la Blockchain est autoportante et autonome.

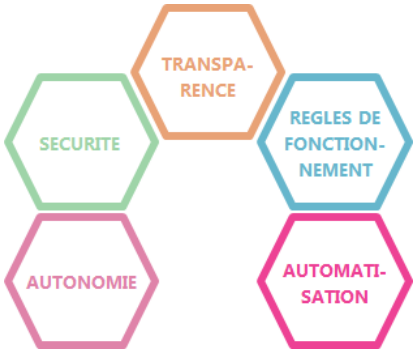
Cette monnaie virtuelle ou 'crypto currency' est personnifiée en grande partie par le célébrissime Bitcoin mais on en dénombre beaucoup plus, environ une centaine, parmi lesquelles on peut également citer l'Ether ou le Ripple (respectivement crypto-monnaies des plates-formes Ethereum et Ripple).

La médiatisation de la technologie a conduit à une montée des activités spéculatives autour de ces crypto devises, pour un encours actuel autour de 330 Mds de dollars [(1)] à fin janvier 2018 ! On peut même estimer que le 'pic' du Bitcoin encore plus vertigineux que celui de la tulipe précédant la Tulipomanie du 17ème (bulle des cours de la tulipe).

EN SYNTHÈSE

Nous avons vu plus haut les principes directeurs qui fondent la technologie Blockchain.

- **La Blockchain garantit la sécurité et l'inaltérabilité des informations** grâce à l'architecture distribuée et l'utilisation de procédés cryptographiques,.
- **La Blockchain distribue la fonction de contrôle et remplace la validation centralisée par le consensus**. A travers le concept de consensus, l'ensemble des nœuds qui constituent la Blockchain participe au processus de validation et empêche de manière collective l'insertion d'informations frauduleuses. Ce consensus ou validation collective rend caduc le contrôle par une institution de référence.
- **La Blockchain ne dépend pas d'un tiers pour disposer des ressources nécessaires à son fonctionnement.** Chaque nœud la constituant est incité à fournir la puissance de calcul et l'espace de stockage requis. Chaque nœud est rétribué par l'octroi de crypto-monnaie, monnaie virtuelle générée par la plate-forme. La Blockchain fonctionne de manière autonome et rémunère les coûts d'infrastructure par la création d'une crypto-monnaie.



(1) Source: www.boursier.com

Les 3 différents modèles de Blockchain

03

Il existe différents modèles de mise en œuvre de la technologie Blockchain. Historiquement, les premières plates-formes Blockchain étaient accessibles à tout utilisateur sans restriction d'accès.

Dans ce **modèle public**, chaque utilisateur est libre de consulter les informations enregistrées sur le registre et d'en publier de nouvelles qui seront elles-mêmes enregistrées tant que les règles de fonctionnement du réseau sont respectées

Le réseau fonctionne de manière totalement décentralisée et autonome grâce au mécanisme de consensus présenté au chapitre deux (2).
L' implémentation la plus connue de ce modèle est la plate-forme Bitcoin.

D'autres modèles existent toutefois.

S'ils se basent sur les même principes d'architecture technique (réseau distribué, organisation des informations par bloc), ils diffèrent toutefois du modèle public en restreignant l'accès au réseau et les droits des différents utilisateurs.

On parle de modèles permissionnés ou 'permissioned ledger' et on distingue deux sous types d'architecture au sein de cette catégorie.

Dans le **modèle consortium**, l'accès au réseau est public mais une gestion des droits permet de restreindre l'accès et l'ajout d'informations.

La gestion de ces droits implique l'existence d'un ou plusieurs utilisateurs ayant un rôle d'administration et de contrôle, c'est pourquoi on parle également de modèle partiellement décentralisé ou de modèle hybride.

Dans le **modèle privé**, les droits d'accès et d'écriture sont centralisés sous la responsabilité d'une seule organisation. Cette organisation contrôle également les règles de fonctionnement du réseau et peut décider de les modifier à tout moment. Les différents mécanismes de confiance introduits par la Blockchain publique (consensus...) ne sont pas ou plus nécessaires car la gestion et le contrôle du réseau est assuré par l'organisation centrale.

LE PERIMETRE D'APPLICATION

Modèle public

Ce modèle est particulièrement adapté à un contexte C2C ('Customer-to-Customer'). Ouvert à tout utilisateur sans distinction, il permet à un écosystème de fonctionner sans intervention d'un tiers de confiance, permettant ainsi de supprimer les frais et les délais inhérents à cet intermédiaire. Le système est particulièrement résilient car il n'est plus dépendant d'un acteur dont la remise en cause suffirait à fragiliser l'ensemble.

Toutefois, ce modèle implique des contraintes de performance (calculs « lourds » requis par le consensus) et des contraintes de scalabilité très importantes (chaque nœud ayant une copie de l'intégralité des informations du réseau), qui limite à ce stade de la technologie leur déploiement à grande échelle.C'est pourquoi, à l'exception du Bitcoin, la plupart des modèles publics sont encore au stade de l'expérimentation et du 'proof of concept'.

Le modèle consortium (hybride)

Le modèle consortium va davantage s'appliquer à un contexte B2B (Business-to-Client), B2C (Business-to-Customer). L'accès au réseau reste libre mais l'accès aux informations est retreint comme la possibilité d'en publier de nouvelles.

Le modèle consortium n'est donc pas totalement distribué, certains utilisateurs ayant le pouvoir d'attribuer, modifier ou révoquer les droits accordés aux utilisateurs restants mais également la possibilité de modifier les règles de fonctionnement du réseau.

Ce modèle réintroduit partiellement le concept de tiers de confiance, les utilisateurs ayant dans ce cas les droits d'administration, ce qui permet de limiter les impacts en termes de performance et de scalabilité des modèles publics. En effet, ces modèles limitent le consensus aux seuls utilisateurs administrateurs ou encore stockent l'intégralité des informations auprès d'eux seulement. L'enjeu de ce type de modèle est davantage de garantir la sécurité et la traçabilité des transactions, la Blockchain garantissant la fiabilité et l'inaltérabilité des informations.

Mais également de faciliter la digitalisation et l'automatisation des opérations grâce notamment aux 'smart contract'. Plusieurs initiatives basées sur ce type de modèles sont en cours, particulièrement au sein de l'industrie bancaire.

Le consortium WeTrade [(1)], fondé par 9 banques européennes et visant à créer une place de marché pour l'exécution des opérations de commerce international est un exemple d'application de ce type de modèle.

Le modèle privé

Dans ce modèle, les droits d'accès au réseau et aux informations sont restreints sous la responsabilité d'un seul utilisateur ou d'une seule organisation.

Ce modèle garantit toujours la fiabilité et l'auditabilité des informations mais les mécanismes de consensus deviennent inutiles du moment que la fonction de contrôle redevient totalement centralisée. On s'éloigne sensiblement du concept initial de la Blockchain et la pertinence de ce type de modèle peut être difficile à évaluer comparé à une classique base de données distribuée par exemple.
Certaines organisations ont toutefois fait le choix d'expérimenter ce type de modèle pour faciliter l'intégration de leurs données. A titre d'exemple, Crédit Mutuel Arkea utilise ce type de modèle pour partager et fédérer les informations de ses clients entre les différentes entités du groupe et faciliter ainsi le process de KYC [(2)]. BNP Paribas a également mis en œuvre un pilote de Blockchain privée pour optimiser sa trésorerie et établir une vision partagée des positions de liquidité dans les différentes implantations de BNP Paribas dans le monde. [(3)]

(1) www.we-trade.com

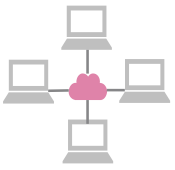
(2) www.finyear.com/IBM-et-Credit-Mutuel-Arkea-pionniers-dans-l-utilisation-de-la-Blockchain-pour-le-KYC-Know-Your-Customer_a36608.html

(3) www.coindesk.com/bnp-ey-complete-blockchain-trial-for-internal-treasury-operations

Public	Hybride	Privé

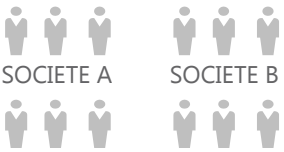
Usage typique

Public	Hybride	Privé
Services Décentralisés C2C	Consortium d'entreprise Partenaires B2B, B2C	Liaison base de données internes Optimisation interne



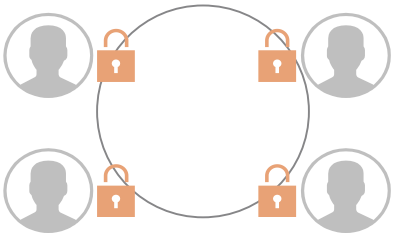
Transparence des participants

Public	Hybride	Privé
Participants Anonymes	Participants identifiés	1 participant identifié



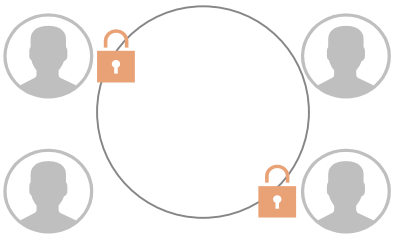
Accès au registre

Public	Hybride	Privé
Ouvert à tous	Restreint aux participants	1 seul acteur



Validation des transactions

Public	Hybride	Privé
Ouvert à tous	Restreint à certains participants	1 seul acteur



Les cas d'usage

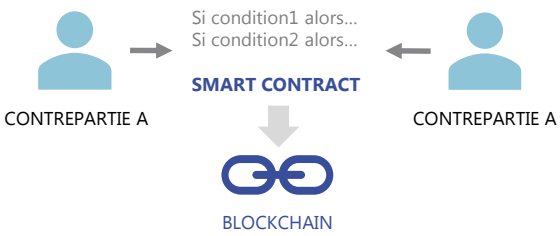
04

LES 'SMART CONTRACTS'

Les smart contracts ou contrats intelligents représentent un des cas d'usages les plus prometteurs de la Blockchain. Ce sont des programmes informatiques reposant sur la technologie Blockchain et conçus pour exécuter automatiquement les termes d'un contrat dès lors que certaines conditions sont réunies.

Ces programmes sont accessibles et auditables par toutes les parties autorisées, leur exécution est donc contrôlée et vérifiable. Enfin, la Blockchain garantit la fiabilité et l'immuabilité de ces contrats.

En automatisant de façon inaltérable les conditions d'exécution d'un accord, ces smart contrats permettent à deux contreparties de nouer un accord commercial sans se faire confiance au préalable et sans nécessiter l'intervention d'une autorité centrale. Grace à ces contrats et à la technologie Blockchain, la fonction de confiance n'est plus portée par les agents du système mais par le système lui-même, de manière totalement automatisée.



Pour louer un appartement par exemple, un smart contract pourrait automatiquement générer une clé virtuelle sur Smartphone dès que le paiement effectué par le locataire est enregistré et authentifié par la Blockchain. A expiration du contrat de location, le smart contract invalide automatiquement cette clé virtuelle.

Un autre cas d'exemple dans le secteur de l'assurance est « Fizzy » (www.fizzy.axa) un service développé et commercialisé par Axa permettant de couvrir les retards d'avion et basé sur ce type de contrat. Concrètement, ce smart contract est connecté au trafic aérien mondial de manière à récolter les informations d'atterrissage des vols. Une fois l'information disponible dans la Blockchain, c'est le smart contract qui prend la décision d'indemniser le client ou non. Si un retard de plus de deux heures est constaté, l'indemnisation se déclenche automatiquement.

Autre exemple de smart contract : le projet 'WeTrade' (www.we-trade.com) qui vise à développer une plate-forme destinée au négoce international. Cette plate-forme permettra d'automatiser les paiements à destination des fournisseurs dès lors que la plate-forme aura été notifiée de la livraison des marchandises.

Note : Si la Blockchain garantit l'inaltérabilité des smart contracts, il reste à confirmer que le code informatique du smart contract reflète exactement les termes du contrat initial. Certaines plates-formes de registres distribués comme Corda permettent d'instancier leurs smart contracts à partir de contrats ricardiens. Ce sont des contrats légaux rédigés de telle sorte qu'ils puissent être automatiquement transposés en langage informatique afin de garantir une exécution rigoureusement identique au contrat initial.

PRINCIPAUX BÉNÉFICES DES SMART CONTRACTS

1. **Revue en temps réel :** les documents financiers étant accessibles via la plateforme, le délai avant expédition de la marchandise est réduit.
2. **Transparence des moyens :** les factures accessibles par la plateforme offrent une vue transparente sur le financement induit à court terme.
3. **Désintermédiation** : les banques facilitent l'opération de trade finance par la plateforme, ce qui rend inutile l'intermédiation par une banque tiers qui doit assumer le risque.
4. **Baisse du risque de contrepartie** : les exemplaires du connaissement sont accessibles via la plateforme, éliminant le risque de dédoublement potentiel de la dépense.
5. **Décentralisation de l'exécution du contrat** : quand les termes du contrat sont remplis, le statut est mis à jour par la plateforme, ce qui réduit le temps et la main d'œuvre nécessaires pour piloter la livraison de la marchandise.
6. **Preuve de propriété :** le droit de propriété est disponible via la plateforme renseignant avec transparence le lieu et la propriété de la marchandise.
7. **Règlement automatique et réduction des frais de transaction** : les termes du contrat sont exécutés via le smart contract éliminant le besoin d'une banque intermédiaire ainsi que des coûts de transaction additionnels.
8. **Transparence réglementaire:** les régulateurs ont accès en temps réel aux documents essentiels à la lutte contre le blanchiment d'argent.

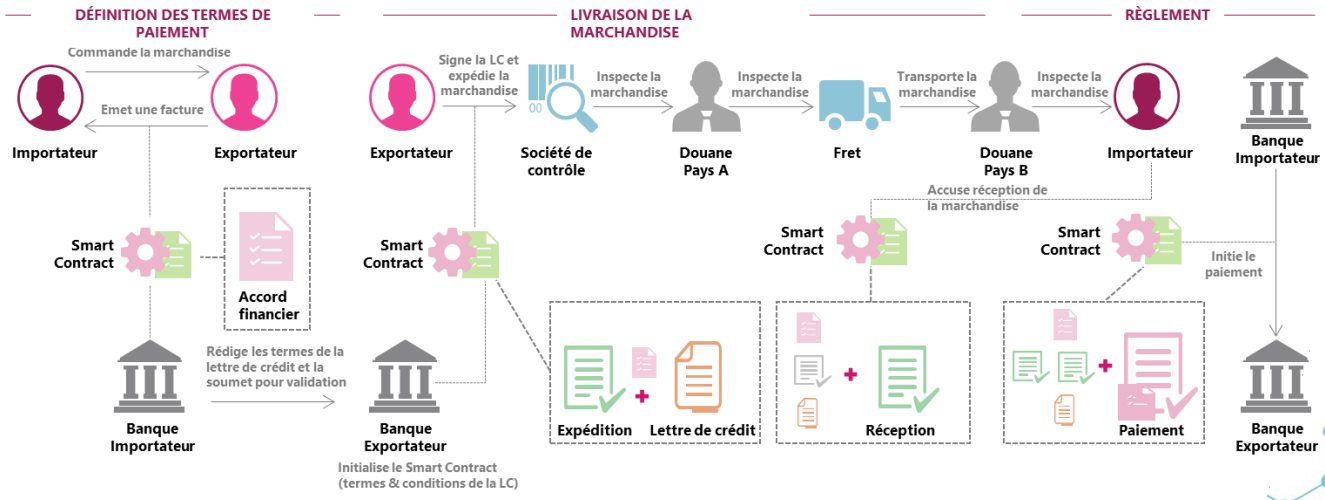


Illustration : Utilisation de Smart Contracts dans une opération de Commerce International

Note : Les smart contracts s'exécutent dès lors que certaines conditions sont respectées. En fonction des situations, ces conditions peuvent être extérieures à la Blockchain et il convient de garantir leur fiabilité au même titre que le smart contrat lui-même. Certaines plates-formes comme Ethereum prévoient des mécanismes ou « Oracles » : un tiers de confiance préalablement désigné par les deux parties du contrat ou encore un service habilité à définir quelles conditions sont considérées valides.

Autre élément non négligeable, en prévoyant des protocoles qui se déclenchent dès que les termes du contrat sont rompus, ces smart contracts laissent envisager une gestion des contentieux beaucoup moins lourde pour les entreprises. Ces perspectives ont poussé de nombreuses organisations à prioriser ce type de projet en particulier au sein du secteur financier.

LES ORGANISATIONS DECENTRALISÉES AUTONOMES

Une organisation décentralisée autonome (ou DAO) est une organisation qui repose sur un programme informatique inscrit dans la Blockchain. Les règles de gouvernances sont décrites par le code informatique et ces règles sont transparentes et immuables car inscrites dans la Blockchain. Par rapport à une organisation traditionnelle, une DAO apporte trois éléments nouveaux.

1. Une DAO fonctionne en permanence, elle ne peut pas être arrêtée sauf si ce cas est prévu en amont lors de sa conception.
2. Une DAO ne peut pas être contrôlée par une personne ou une entité. En particulier, les règles ou les données ne peuvent être modifiées à des fins frauduleuses.
3. Les règles de fonctionnement d'une DAO sont transparentes et auditables

Un exemple de DAO est le projet 'OpenBazaar' (www.openbazaar.org), une place de marché similaire au Bon Coin fonctionnant de manière autonome et ne générant aucun coût, donc totalement gratuit pour l'utilisateur.

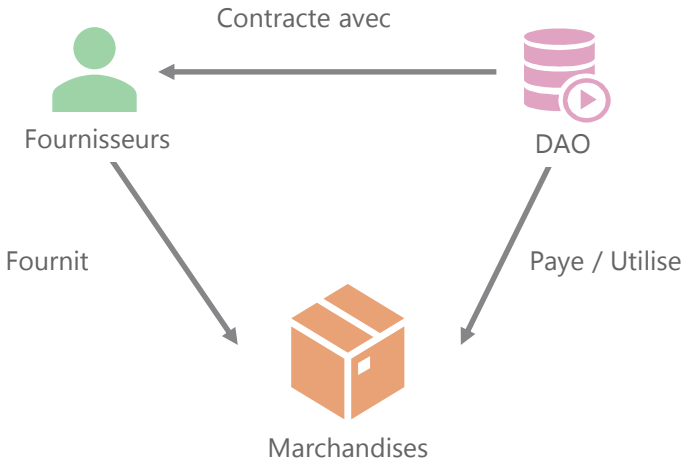


Illustration : Fonctionnement d'une DAO

LA BLOCKCHAIN ET L'INTERNET DES OBJETS

L'Internet des objets va probablement constituer un des vecteurs majeurs d'adoption de la technologie Blockchain.

Les chiffres sont éloquents : d'ici 2020, on estime que le marché de l'Internet des objets ou IOT représentera 7 100 milliards de dollars et 50 milliards d'objets seront connectés à Internet. La masse d'information que cela représente est gigantesque et bien évidemment, le premier enjeu de l'IOT est de garantir la fiabilité et la sécurité de ces informations.

Mais la Blockchain peut permettre d'aller plus loin et servir de socle à la construction d'une organisation autonome qui permettrait à ces objets d'interagir entre eux sur la base de smart contracts.

L'intérêt est ici d'intégrer de façon totalement automatisée cette masse d'information dans une chaîne de valeur économique. La Blockchain permettrait de garantir la sécurité et la fiabilité des informations et, grâce aux gains de coût, ouvrirait la voie à la création de nouveaux modèles économiques basés sur une exploitation automatisée de ces informations.

Dans le secteur de la distribution par exemple, la startup Filament (www.filament.com) travaille actuellement sur la mise en place d'une Blockchain couplée aux objets connectés pour optimiser le suivi et la gestion des stocks d'inventaire.

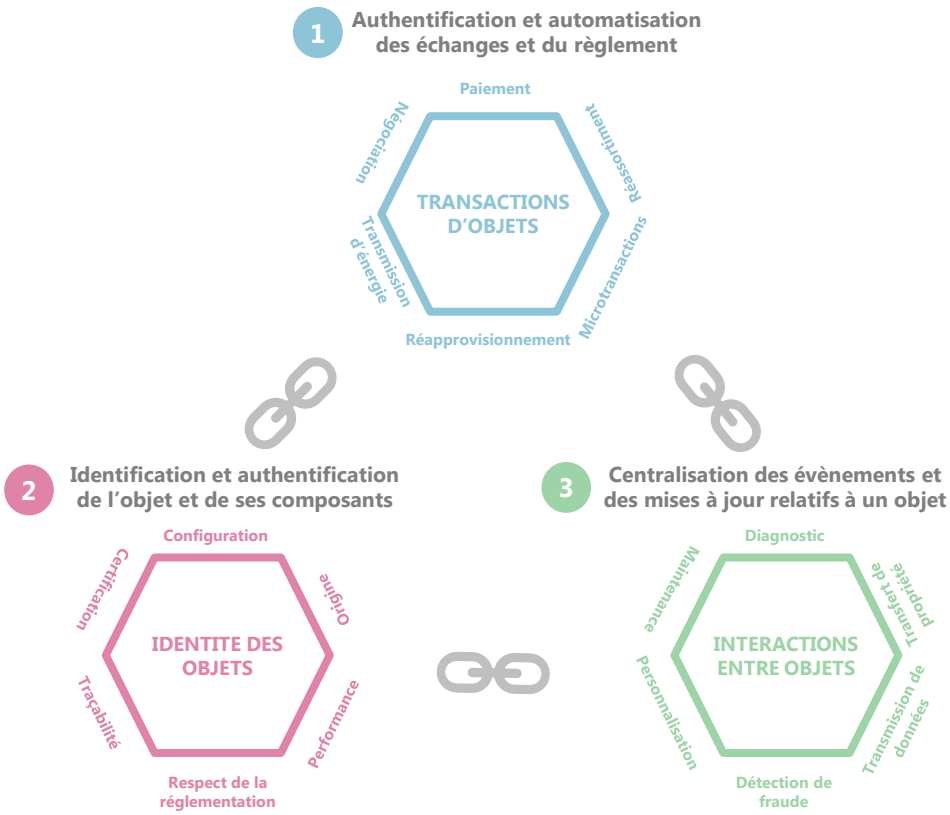
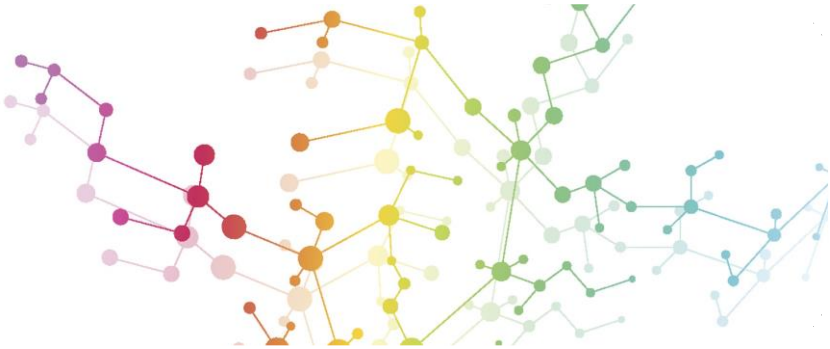


Illustration : Blockchain & IOT

Du modèle à la réalité : quelles contraintes ?

05



A l'exception de la Blockchain Bitcoin et dans une moindre mesure d'Ethereum, l'ensemble des initiatives basées sur Blockchain restent encore au stade de l'expérimentation, ou sont sinon déployées sur une échelle relativement limitée. Comme pour toute nouvelle technologie, de nombreuses contraintes et limitations nécessitent d'être solutionnées avant d'envisager un déploiement sur une échelle industrielle.

LA QUESTION DE LA SCALABILITE

La première contrainte est liée à la capacité de la technologie à supporter un usage industriel en gérant un volume important de transactions dans un laps de temps réduit.

La réponse est loin d'être évidente à ce stade. A titre d'exemple, les performances de la Blockchain Bitcoin – 7 transactions par seconde (1) – sont loin des standards attendus pour une utilisation industrielle. Par comparaison, le réseau VISA est capable de gérer des pics à 55 000 transactions par seconde.

Toutefois, le nombre d'expérimentions en cours sur cette technologie, les investissements prévus dans de nombreux secteurs d'activité et la richesse de l'écosystème technique (start-up, communautés de développeurs…) nous laisse raisonnablement penser que cette contrainte ne devrait plus l'être à court voir moyen terme.

LA FACILITE D'INTEGRATION

À l'heure actuelle, intégrer une couche Blockchain dans une architecture reste une tâche complexe.

Le coût technique n'est pas neutre, d'autant que les compétences requises sont rares sur le marché. Or, cette technologie a vocation à être un socle technique sur lequel viendront se greffer des composants porteurs de la logique métier, de manière similaire à un système d'exploitation qui permet à des applications dédiées de fonctionner (tableur, éditeur de texte).

Pour pallier cette problématique, plusieurs éditeurs informatiques commencent à structurer des offres 'Blockchain as a Service' ou BaaS.

Ce sont des offres sur le Cloud permettant de développer des services basés sur la Blockchain sans avoir à investir dans une infrastructure ad hoc. L'objectif est de masquer la complexité technique de la Blockchain et de laisser les utilisateurs se concentrer sur le développement de composant centrés sur leur cœur de métier.

Si ce type de service est récent et encore cantonné à des phases d'expérimentation, il devrait assez rapidement être en mesure de basculer dans une phase industrielle.

(1) Source: www.latribune.fr - Janvier 2018

COMPARATIF DES OFFRES DE BaaS (BLOCKCHAIN AS A SERVICE)

Editeur / solution	Année de lancement	Plateformes prises en charge	Modèle tarifaire	Références
HPE	Début 2018	R3 Corda	NC	NC
IBM / IBM Blockchain	Février 2016	Hyperledger Fabrid version 1O	752 €/mois	Bank of Tokyo, Mitsubishi UFJ, Northern Trust
Microsoft / Blockchain sur Azure	Novembre 2015	Ethereum, Hyperledger Fabric, R3 Corda, Chain Core…	Lié au stockage, au compute et à la consommation de services cloud	
SAP / Leonardo Blockchain	Mai 2017	Pogramme Leondardo	NC	NC

(*) source : le Journal du Net

LA QUESTION DU BUSINESS MODEL

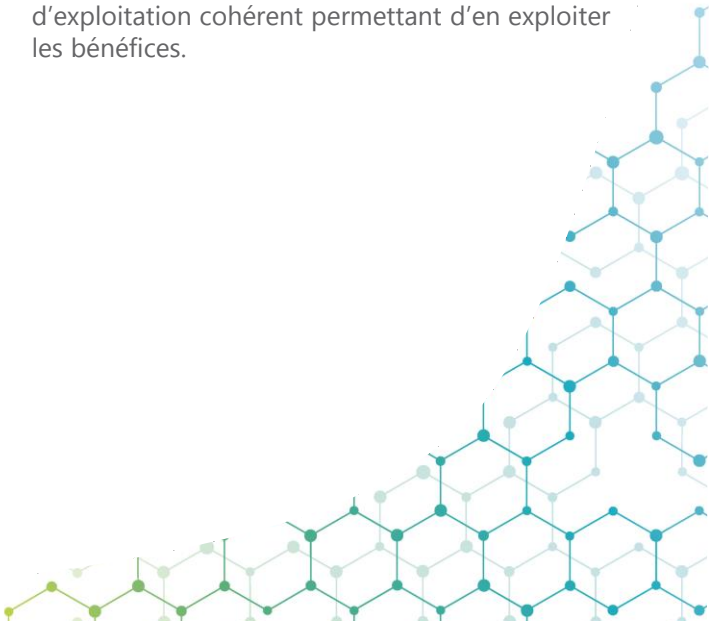
En complément des contraintes techniques, une autre contrainte est liée à la difficulté de trouver un business model adéquat. Une première raison, liée à la maturité de la technologie, tient au fait qu'il n'existe pas de standards permettant d'interconnecter plusieurs Blockchains entre elles au sein d'une chaîne de valeur unique.

Une deuxième raison est liée à l'absence de cadre juridique clair. De nombreuses initiatives et travaux ont été et sont encore initiés par les différents régulateurs mais ceux-ci restent encore très localisés à un état ou une zone géographique, ce qui empêche ou du moins complexifie fortement la perspective d'un déploiement international d'un service basé sur cette technologie. Nous abordons ce point plus en détail en chapitre 6.

Enfin une troisième principale raison est liée à la problématique de gouvernance. La plupart des projets Blockchain en cours, principalement au sein de l'industrie financière, s'organisent autour d'un modèle de consortium qui n'est pas sans poser de fortes problématiques de gouvernance.

En effet la question du partage des données client ou de gestion des droits entre les différents membres du consortium pose de nombreuses contraintes aux établissements qui avaient jusqu'alors plutôt l'habitude de travailler en vase clos et d'avoir un contrôle total sur la relation client.

Si la Blockchain offre des perspectives indéniables en terme d'optimisation opérationnelle et de digitalisation, reste encore à définir un modèle d'exploitation cohérent permettant d'en exploiter les bénéfices.



Les impacts organisationnels

06

La rupture fondamentale de la technologie Blockchain est d'introduire de la confiance dans un réseau pair à pair anonyme, c'est à dire la possibilité de fixer un 'contrat' entre deux utilisateurs, de façon fiable et pérenne sans passer par un tiers de confiance. La Blockchain se suffit à elle-même : elle porte en elle-même les preuves qu'un accord a eu lieu et cette preuve est visible de tous et ne pourra plus être modifiée postérieurement.

Autrement dit, elle a le potentiel de remettre en cause les organisations verticales assurant cette fonction de contrôle, au profit d'organisations autonomes décentralisées sans différences entre utilisateurs de services et prestataires de services. Les utilisateurs participent à leur guise à la production, grâce à l'éclatement de toutes les activités en opérations distinctes que chacun entreprend de réaliser selon ses possibilités et ses motivations.

UN MODE DE TRAVAIL DÉCENTRALISÉ… À TERME

La plateforme Blockchain Ethereum reprend les mêmes bases que la Blockchain Bitcoin (consensus distribué, validation cryptographique des opérations) mais rajoute à ce socle la possibilité d'échanger n'importe quoi via l'introduction des smart contracts décrits plus haut.

Ethereum permet d'échanger de la valeur, des modalités contractuelles, en stockant du code dans la Blockchain, de l'exécuter et d'en apporter les preuves d'exécution.

Comme le décrit son cofondateur Joseph Lubin, Ethereum est un « ordinateur à but général » (general purpose computer) et un « substrat pour construire des systèmes économiques, sociaux et politiques globaux qui soient transparents, configurables de manière privée, profondément sécurisés, non censurables, non répudiables et nativement interopérables ».

Dans la vision de Joseph Lubin, à l'avenir chaque entreprise définira ses processus au sein d'une Blockchain privée et les entreprises interagiront entre elles, ou plutôt leurs Blockchains respectives communiqueront entre elles via la plateforme publique Ethereum.

Mais ce qui vaut pour les entreprises vaut également pour les individus qui pourraient à travers cette plate-forme s'organiser en réseau, contribuer collectivement à la création de valeur et être rétribués en fonction de leur contribution sur la base de règles prédéfinies et acceptées par tous. Pour illustrer ces nouveaux modes d'organisation décentralisée, on peut citer le projet Arcade City équivalent à Uber mais sans Uber. C'est un service de covoiturage, développé sur la plateforme Ethereum fonctionnant sans intermédiaires, les trajets étant automatiquement enregistrés et rétribués par la plate-forme.

Cette technologie est un levier prometteur à la mise en place de systèmes économiques collaboratifs et cohérents capables de générer de la valeur, et de la distribuer équitablement entre tous les participants.

UNE ÉVOLUTION DE LA GOUVERNANCE

Au-delà des expérimentations d'organisations autonomes et décentralisées, le deuxième axe de changement organisationnel concerne le mode de gouvernance. La Blockchain promet non seulement de créer de nouvelles formes organisationnelles mais surtout l'émergence de structures qui pourront fonctionner sans intermédiaires.

Dans une Blockchain privée aussi bien que publique, une organisation se caractérise par un ensemble de relations contractuelles entre les acteurs. La bonne exécution des contrats est assurée par des protocoles informatiques (les 'smart contracts') dont la souplesse permet d'y intégrer les modalités de gouvernance.

A travers cette gestion informatique de la confiance se crée un biais inhérent à un intervenant qui chercherait à mettre en avant ses propres intérêts. En complément, il n'y a plus de surcoût lié à des frais de transaction, ni à des mécanismes de contrôle ou à des politiques d'incitation (à respecter les règles).

Mais quid du pouvoir détenu par ceux qui en assurent le contrôle, c'est-à-dire ceux qui écrivent les règles ? Si la définition des règles revient en effet à régir l'ensemble de la chaîne ('Code is Law'), il ne sera pas toujours suffisant de proposer à tous les acteurs la sécurité et l'auditabilité du code. Encore faut-il que ces tâches de surveillance/supervision soient réalisées… C'est pourquoi des organismes indépendants de contrôle et de régulation pourront être nécessaires pour assurer un contre-pouvoir.

Dans la sphère financière, ces systèmes préfigurent surtout la prochaine génération d'infrastructures, permettant aux principaux acteurs et aux régulateurs d'accéder à des tableaux de bord en temps réel. Ces évolutions ne seront vraiment valables que lorsque la Blockchain y aura pris une place considérable et que la réglementation aura évolué. Ce qui est loin d'être le cas…

Pour le moment, l'AMF plaide pour une Blockchain ouverte et réglementée permettant au régulateur d'accéder à certains nœuds de la chaîne pour contrôler les données. De son côté, la BCE, après une étude d'une année sur des livres comptables distribués, a considéré que la technologie n'était pas assez mûre pour relever les principaux défis bancaires institutionnels et remplacer des applications à grande échelle telles que TARGET2.

Si la technologie n'est pour le moment pas considérée comme assez robuste, les instances de régulation ont tout de même volonté d'aller beaucoup plus loin et de se pencher sur le fonctionnement des DLT à ce stade de leur développement. Ce qui permettra d'intégrer nativement des mécanismes de gouvernance et de réglementation au sein de la technologie.

L'ÉMERGENCE DE NOUVEAUX MÉTIERS

Dans un troisième temps, ce sont les compétences en lien avec les processus qui seront impactées. Dès lors que la technologie va automatiser les opérations et faciliter l'audit / le contrôle des règles ainsi que leur respect par les parties prenantes, les tâches à valeur ajoutée vont se concentrer sur la mise en qualité de la chaîne. Autrement dit, si la chaîne assure elle-même de manière native le contrôle des opérations, il conviendra désormais de contrôler les programmes qui exécuteront ces opérations.

Avec la Blockchain, il est possible d'horodater les contributions de chacun et d'en conserver un historique, essentiel dans une organisation agile et ouverte. Cela va donc simplifier les tâches de contrôle et d'audit en facilitant le tracking mais faire apparaître de nouveaux métiers liés à la définition / au checking / à la certification du modèle :

- des profils juridiques / audit capables de lire le code, d'en comprendre les impacts métier et de déceler d'éventuelles erreurs (avec l'éventuel appui d'outils IT)
- des experts sécurité capables de garantir l'intégrité des composants de la chaîne
- des contrôleurs qualité capables de réaliser un audit ou une mesure du risque en temps réel
- des responsables métier capables de concevoir et faire évoluer les processus en les intégrant dans les Smart Contracts

Finalement, contrairement à l'idée reçue, nous pensons que l'adoption de cette technologie dans nos organisations professionnelles ou sociales va passer par un renforcement des fonctions de contrôle et de supervision visant à garantir l'intégrité de la chaîne.

UNE ÉVOLUTION QUI POSE DES QUESTIONS

Si la Blockchain est une technologie complexe, ses impacts le sont encore plus. Elle a le potentiel de favoriser l'émergence d'organisations plus collaboratives et participatives mais elle soulève nombre de questions juridiques et éthiques sur le rôle que doit jouer la technologie dans nos interactions sociales. Nous pensons que cette technologie va probablement changer nos organisations mais elle le fera graduellement comparé à son pouvoir disruptif.

Enfin, paradoxalement, cette transformation ne pourra se faire qu'au travers d'un renforcement des fonctions de régulation et de contrôle qui pour certaines d'entre elles restent à inventer.

Nous pensons en particulier que le secteur juridique sera concerné par ces évolutions car il sera nécessaire de développer des compétences capables d'apporter une validité légale à des codes informatiques.

Les impacts juridiques

07

En l'état actuel, la technologie se développe beaucoup plus rapidement que le droit n'évolue. A ce jour, le cadre juridique sur la Blockchain reste flou, malgré quelques initiatives locales pour tenter de la réguler.

Quelle validité juridique pour les opérations réalisées sur la Blockchain ? Quelles conditions de rétroactivité ? Comment gérer la confidentialité des données lorsque cela est nécessaire ? Ces questions comme de nombreuses autres restent en l'attente de réponses, particulièrement pour les modèles publics.

LA BLOCKCHAIN, UNE TECHNOLOGIE PEU CONTRÔLÉE

La Blockchain est une technologie qui porte de nombreux espoirs, tant par les nouveaux produits et services qui se mettent en place, que par les possibilités qu'elle laisse entrevoir. Cependant, certains investisseurs restent frileux à s'y engager, redoutant les zones de flou juridique que cette nouvelle technologie a créées.

Ainsi dans le cas d'une Blockchain publique, une question de responsabilité est mise en avant, et ce pour plusieurs raisons :

Les transactions sont anonymes ou pseudo-anonymes. Le « Know Your Customer » obligatoire aux organismes financiers y est souvent absent ou limité. Ce processus de contrôle permet aux établissements financiers de récolter certaines informations sur les interlocuteurs avec lesquels ils devront traiter.

Ils peuvent ainsi s'assurer que ces derniers ne sont pas impliqués dans des activités comme le trafic d'armes ou bien n'ont pas de relation avec des pays sous embargo ou sanction financière. De la même façon, le « Know Your Transaction » permet aux établissements financiers de s'assurer de l'origine des fonds qu'ils reçoivent. Cette absence de contrôle, inscrite dans le protocole de fonctionnement de la Blockchain, nourrit nombre d'inquiétudes liées aux problématiques de fraude, de blanchiment d'argent, de contournement des sanctions financières ou des embargos.

La plateforme une fois mise en place n'est pas administrée. L'administration est intégrée dans le code.

Cela suppose que le code ne contienne pas de faille pouvant mener à une mauvaise exécution des ordres. Ainsi récemment, les failles d'un smart contract d'Ethereum ont permis à un utilisateur de recevoir plusieurs dizaines de milliers d'euros. Cela suppose que la Blockchain se substitue à l'humain pour ce qui est du pouvoir de décision et pose donc des problématiques éthiques. Pour reprendre l'expression de Primavera de Filippi, chercheuse à Harvard et au CNRS, « faire du code c'est déjà faire de la politique ». En effet, si la Blockchain doit structurer les échanges de demain, ses mécanismes devront être pensés non seulement pour assurer une distribution du pouvoir de décision mais aussi garantir un respect des valeurs morales.

Cela suppose aussi que le code initial de la plateforme soit capable de gérer tous les évènements à venir sans création de litige. Par exemple, l'exécution automatique d'un testament par un smart contract ne tiendra pas compte d'un événement imprévu et il faudra alors se poser la question de réparer le dommage dans un système supposé immuable. Les smart contracts ne peuvent pas prévoir toute circonstance exceptionnelle pouvant interférer dans l'exécution d'un contrat classique et malgré cela, ces contrats ont pour principe de s'exécuter automatiquement.

Bien que la Blockchain soit une technologie qui repose sur son inviolabilité, les risques de hacking de la chaîne ne sont pas nuls. Ainsi, les cas de piratage sur des plateformes de cryptomonnaie sont nombreux.

VERS UNE RÈGLEMENTATION DES ÉCHANGES

Les réactions vis-à-vis de la Blockchain sont ainsi partagées entre le désir de laisser la technologie développer son potentiel et le souci d'éviter les dérives. Tel qu'évoqué, la Blockchain présente des risques indéniables, qu'ils soient liés au blanchiment d'argent, au financement d'activités illicites ou à la fraude.

La Chine, de son coté, redoute également la perte de contrôle et une fuite des capitaux. C'est ainsi que, début septembre 2017, elle interdisait les levées de fonds réalisées en crypto monnaies. La Corée du Sud limite également l'échange de cryptomonnaies.

A l'inverse, une majorité des pays privilégie une réglementation modérée qui ne freinera pas le développement de la technologie afin d'éviter de prendre du retard par rapport à la concurrence. Dans ces pays, la Blockchain et plus spécifiquement les crypto-monnaies ne sont pas rendues illégales mais ne bénéficient pas encore d'un encadrement spécifique par le droit.

La France se positionne comme le pays précurseur en termes de réglementation des ICO (devant Malte ou la Suisse). Pour pouvoir peser demain dans ces émissions initiales de jetons, Le Trésor et l'Autorité des Marchés Financiers se sont impliqués dans la définition de standards. Le **projet de loi Pacte** qui devrait entrer en vigueur début 2019 a pour objectif de jeter les bases de ces nouveaux modes de financement et ainsi de renforcer l'attractivité de la Place de Paris.

L'encadrement des levées de fonds en crypto-actifs sera alors assuré par la délivrance d'un visa optionnel par l'AMF (pour les Utility Tokens). Ce qui permettra d'attirer les bons projets à l'échelle internationale, de les rendre plus crédibles (sans garantie quant à leur solidité) dans un cadre relativement souple et rassurant pour les investisseurs (prospectus d'émission, mécanisme de sauvegarde des fonds levés). Ce dispositif aura également comme avantage de limiter les cas de fraude et d'assurer la vérification de l'origine des fonds et de lutte contre le blanchiment.

Note : Le point noir reste la fiscalité avec jusqu'à 70% d'impôt sur la plus-value réalisée sur les crypto-actifs (à déclarer en BIC ou BNC). Pour devenir une Place de référence dans ce domaine, la France devra donc rendre son traitement fiscal plus attractif.

UN CADRE ENCORE INSUFFISANT SUR LA CONFIDENTIALITÉ DES DONNÉES

Sur ce point, la question est de savoir si les données stockées sur la Blockchain relatives aux utilisateurs peuvent être analysées et récupérées à leur insu. En effet, la Blockchain a pour principe la transparence et le caractère distribué : chaque utilisateur possède potentiellement une copie de la base de données. Il convient donc de s'assurer que certaines données soient suffisamment protégées. On pense par exemple aux transactions réalisées par une entreprise, qui pourraient révéler sa stratégie. Des initiatives récentes permettent de résoudre cette problématique, que ce soit l'ajout d'une fonctionnalité spécifique à la Blockchain (société Blockstream) ou par l'intégration native de la confidentialité dans la solution (plate-forme Hyperledger).

QUELLES VALIDITÉS JURIDIQUES POUR LES TRANSACTIONS BLOCKCHAIN

Trois principaux critères entrent en ligne de compte dans la validité juridique des opérations réalisées sur une Blockchain.

Le type de Blockchain

La question de la légalité des opérations ne se pose pas de la même façon pour les différents types de chaînes. Elle ne se pose pas pour une Blockchain privée, puisqu'il n'y a qu'un seul acteur. S'agissant d'une Blockchain semi-privée, les participants étant par définition limités, ceux-ci peuvent s'accorder sur la valeur juridique des opérations. Pour une Blockchain publique, les transactions n'ont pas de valeur légale dans le sens où elles ne sont pas opposables au tiers, à moins d'un encadrement spécifique par le droit.

Le pays

Si la plupart des pays ne considèrent pas la Blockchain ni l'échange de crypto-monnaies comme illégaux, très peu de pays ont explicité dans le droit la valeur juridique des transactions effectuées sur une Blockchain afin de protéger ses utilisateurs.

La France est un des rares pays où l'ordonnance du 28 avril 2016 dédiée au 'minibons' permet de rendre les transactions de crypto-monnaies opposables au tiers. Puis l'ordonnance 'Macron' du 8 décembre 2017 a permis l'utilisation d'un dispositif d'enregistrement électronique partagé : adaptation du Code de Commerce et du Code Monétaire et Financier pour permettre d'inscrire l'émission ou la cession de titres financiers dans une Blockchain.

Les déclinaisons de la Blockchain

L'enjeu de la **validité juridique d'opérations effectuées sur la Blockchain** n'est pas le même selon qu'il s'agisse d'un « jeton utilitaire » (**Utility Token**) ou d'un « jeton d'authentification » (**Security Token**).

Le jeton utilitaire est un outil dont les fonctionnalités sont de payer (il s'agit alors de crypto-monnaie), de voter, de donner un avis ou de partager une information… Il permet la mise en œuvre de produits / services intelligents, sécurisés et personnalisés.

Dans ce cas, il ne s'agit que de transfert de données ou d'actifs réels. Les problématiques associées sont connues (confidentialité, responsabilité, cybersécurité) et gérées par le droit commun actuel (droit civil et droit commercial).
Le jeton d'authentification (ou de sécurité) est un actif digital ; il peut être assimilé à un droit de propriété ou un droit financier et doit donc toujours être conforme aux lois et règlements en vigueur. Dans ce cas, la Blockchain correspond à un transfert d'actifs digitaux pour lesquels il n'existe à ce jour pas de réglementation spécifique. Typiquement, tant que ces 'Tokens' ne seront pas considérés comme des actifs financiers, ils resteront en dehors du champ de compétence de l'ESMA.

C'est pourtant déjà le cas aux Etats-Unis où existent des 'crypto-shares' qui sont conformes à la loi sur les valeurs mobilières de 1933 mais n'exigent pas d'agrément de la part du régulateur (SEC).

C'est pourquoi une évolution de notre cadre réglementaire est nécessaire (cf. Loi Pacte). A ce stade, le code monétaire et financier français ne reconnait l'échange de titres que par la notion d'inscription en compte chez un émetteur et la présence d'un intermédiaire lors du transfert. Comme le souligne Europlace dans son livre blanc, la Blockchain ne fonctionnant pas sur ce principe de tenue de compte matérialisé par le débit d'un compte et le crédit d'un autre compte, ses transactions ne sont pas encore reconnues. Il est donc prévu de définir un actif digital et de considérer un enregistrement dans une Blockchain comme équivalent à un enregistrement en compte.

La réglementation, non pas de la technologie elle-même, mais des effets de la technologie (nouveaux types d'actifs) fait encore face à deux questions de taille :

- doit-on envisager un transfert de propriété de l'actif ou simplement une preuve de transfert ?
- qui est responsable de la régulation de l'ensemble ? difficile d'appliquer un droit local ou européen à une technologie globale donc internationale…

En résumé, la technologie Blockchain se développe rapidement, dans un environnement juridique qui demande à être adapté. Si le cadre juridique va certainement se développer sur à moyen terme autour des applications les plus matures ainsi qu'au gré des problèmes rencontrés, la question juridique demeure un enjeu important pour le développement de la technologie. Dans l'immédiat, au regard des risques encourus (investissements à perte, divulgation d'informations, enracinement sur une technologie…), bon nombre d'acteurs restent spectateurs et attendent des plates-formes stabilisées, fiables dans leur fonctionnement et leurs conditions d'utilisation. Certains précurseurs (notamment dans le domaine financier) investissent sur quelques projets, en général plusieurs en parallèle, pour anticiper les problématiques aussi bien techniques que juridiques.

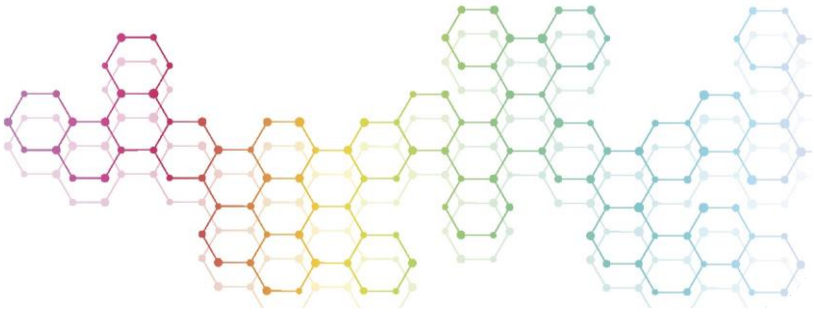
Quant à la réglementation des chaînes publiques, cela passera nécessairement par une législation adaptée, coordonnée et partagée à l'échelle internationale.

Note : A ce jour, 2/3 des Tokens émis sont des 'Utility Tokens' et seulement 13% des 'Security Tokens'... Pourtant, avec des levées de fonds 10 fois plus importantes sur les premiers mois de 2018 qu'en 2017, le marché des 'Security Tokens' devrait rapidement décollé ; il est estimé entre 5 et 10 milliards de dollars à horizon 2023 avec de sérieux avantages sur les marchés traditionnels :

- *place de marché 24 x 7*
- *baisse des coûts de transaction*
- *amélioration des délais de transaction et de règlement*
- *transparence améliorée*
- *faible coût de liquidité*
- *pas de problème de fractionnement*
- *baisse de la corruption (respect des limites réglementaires)*
- *mises à jour dynamiques des aspects contractuels et de gouvernance*
- *valorisation fixée par le marché*
- *accès aux investisseurs facilité*

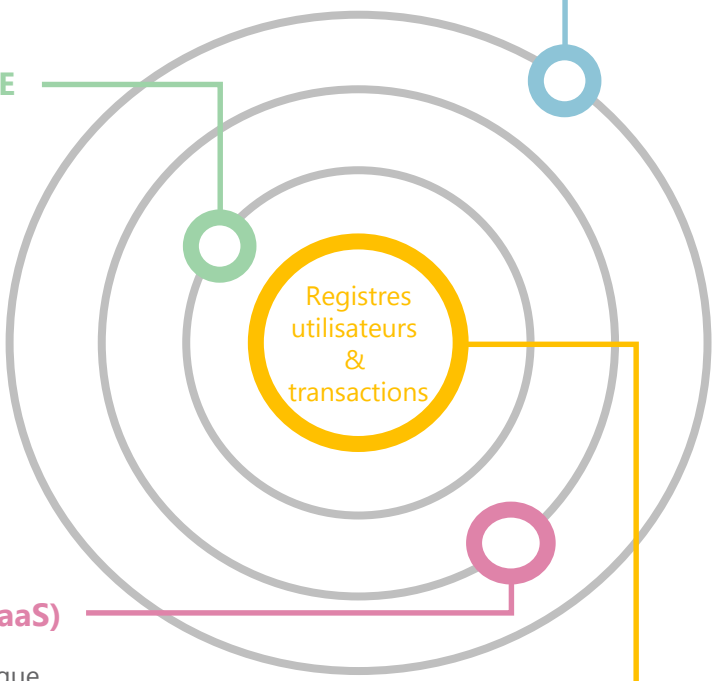
Les fondamentaux techniques

08



Cette partie, dédiée aux aspects techniques de la Blockchain, reprend plus en détail certains concepts évoqués précédemment tels que les différents types de plateformes ou de consensus.

L'écosystème Blockchain



UTILISATEURS

Partis politiques
internationales
Organisations
Associations
Entreprises
Individus
Startups
Etats

COUCHE TECHNOLOGIQUE

Goochain
Backfeed
Stratumn
Factom
Enigma
Ripple
Chain
Linq
Colu
R3

BLOCKCHAIN AS A SERVICE (BaaS)

Crowdfunding
Data storage
Logistique
Assurance
Logistique
Transport
Paiement
Banque
Notariat
Energie
Culture
Media
IoT

BLOCKCHAINS

Ethereum
Bitcoin
Muse
NXT

Tableau comparatif des plates-formes

	Type de Blockchain	Date de création	Type de consensus	Temps de validation des blocs	Gouvernance	Utilisation de smart contracts	Token
Bitcoin	Publique	2008	Proof Of Work	10 minutes	Pas de gouvernance	Non	Bitcoin
Ethereum	Publique	2015	Proof of Work (migration prévue sur Proof of Stake)	Entre 13 et 30 secondes	Fondation Ethereum	Oui	Ether
Hyperledger Fabric	Privée	2015	Practical Byzantine Fault Tolerance	Dès la validation d'une transaction	Fondation Linux	Oui, appelés 'chaincode'	Pas de token
Ripple	Publique	2012	Ripple Protocol Consensus Algorithm	Entre 3 et 5 secondes	Ripple Labs Inc.	Non	XRP
Corda	Privée	2016	Validation par les notaires du réseau	Pas de création de blocs	Consortium R3	Oui	Pas de token
Stratumn	Privée	2015	Proof of process	N/A	Stratumn	Oui	Pas de token

REGISTRE DISTRIBUÉ

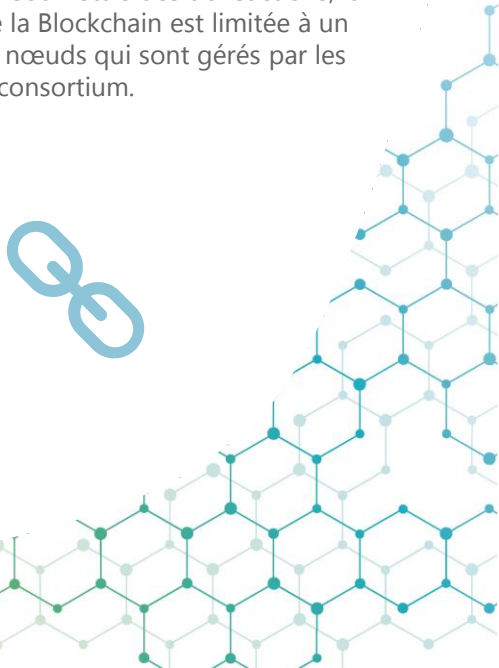
Un registre distribué est un consensus de données numériques reproduites, partagées et synchronisées géographiquement sur de multiples sites, pays ou institutions. Les transactions inscrites sur le registre sont visibles de tous les acteurs du réseau et il n'existe pas d'administrateur central. Pour faire simple, un registre distribué est une base de données décentralisée et répliquée sur un ensemble de lieux géographiques du réseau appelés nœuds. Chaque membre du réseau possédant un nœud a accès à l'historique des transactions passées sur le réseau. La Blockchain est un concept dérivé de la technologie de registre distribué et un fondamental technique des cryptomonnaies comme le bitcoin.

L'information stockée sur le registre est sécurisée au travers d'algorithmes cryptographiques et peut être accédée via l'utilisation de clés et de signatures cryptographiques. Une fois inscrite sur le registre, cette information devient immuable et est soumise aux règles de gouvernance du réseau. L'information est stockée sur des blocs qui sont hashés et encodés.

Chaque bloc contient la signature cryptographique du bloc précédent et tous les blocs de la chaîne sont ainsi liés par un même algorithme. Face aux registres centralisés qui sont vulnérables aux attaques informatiques, les registres distribués sont par nature plus difficiles à pirater car tous les nœuds du réseau doivent être attaqués simultanément.

De plus, ces registres ne peuvent pas être modifiés a posteriori. A titre d'exemple, le réseau bitcoin n'a jamais été piraté depuis sa création en 2009.

Les réseaux Blockchain peuvent être partagés en deux catégories : privés ou publics. Les systèmes open source tels que le Bitcoin ou l'Ethereum sont publics. Ils peuvent être utilisés par n'importe qui. N'importe quel nœud peut valider une transaction et prendre part au processus de consensus pour construire la chaîne de blocs. Les Blockchains privées telles que Hyperledger Fabric & Corda sont destinées à des consortiums au sein desquels la participation est restreinte. Tandis que les clients sont autorisés à soumettre des transactions, la construction de la Blockchain est limitée à un nombre fixe de nœuds qui sont gérés par les membres d'un consortium.



LES CONSENSUS

La sécurité du modèle de consensus est un aspect critique à prendre en compte lors du choix d'une plateforme Blockchain. Le mécanisme de consensus garantit l'inviolabilité de la donnée enregistrée sur le réseau. Un mauvais choix de consensus peut rendre la plateforme inutilisable à cause de la compromission des données. Le registre distribué est mis à jour via un protocole de consensus propre au réseau, et qui permet d'ordonner sans ambiguïté les transactions et de garantir l'intégrité et la cohérence des blocs parmi les nœuds du réseau. Il existe de nombreux consensus dont voici les plus populaires

DESCRIPTION	AVANTAGES	INCONVÉNIENTS
PoW - Proof of Work : Preuve de travail. Dans une Blockchain publique, les ordinateurs des mineurs sont mis à disposition pour résoudre un problème mathématique compliqué. Le 1er qui trouve une solution gagne la récompense du prochain bloc de la chaine (12.5 bitcoin ou 5 ether).	Sécurisé, éprouvé et robuste.	Très consommateur d'électricité et de matériel informatique.
PoS - Proof of Stake : Preuve d'enjeu. Les validateurs de transactions doivent mettre en gage la possession de crypto monnaie pour recevoir une récompense. Si un nœud est malveillant, il peut perdre sa mise en gage au profit des validateurs honnêtes.	Peu consommateur en ressources énergétiques.	Peu testé à grande échelle.
PBFT - Practical Byzantine Fault Tolerant : Consensus dont la liste des validateurs est connue au départ et peut tolérer jusqu'à 1/3 de nœuds compromis (déconnectés ou malveillants).	Consensus de groupe rapide et performant. Pas de fork ou de réorganisation de chaine.	Chaine privée uniquement
PoA - Proof of Authority : Preuve d'autorité. Consensus dont la liste des validateurs est connue au départ et qui valide à tour de rôle un bloc. Ce type de consensus peut tolérer jusqu'à 49% de nœuds malveillants ou déconnectés.	Consensus de groupe rapide	Chaine privée uniquement. Fork ou réorganisation de la chaine possible.

LES PLATES-FORMES

BITCOIN

Le réseau Bitcoin est une plateforme de paiement en peer-to-peer. Il s'agit du premier réseau Blockchain, né en 2008. Les transactions ont lieu entre utilisateurs, sans intermédiation d'un tiers de confiance. Le réseau Bitcoin ne permet pas la mise en place de smart contracts. Techniquement le réseau bitcoin ne permet donc que de recevoir et d'envoyer des transactions.

ETHEREUM

Cette Blockchain créé par Vitalik Buterin a été livrée mi-2015 dans sa première implémentation publique appelée 'Frontier'. Elle est liée à une crypto-monnaie, l'Ether dont sa principale avancée est de permettre la mise en place de smart contracts dans différents langages informatiques.

HYPERLEDGER FABRIC

Hyperledger est un incubateur de projets autour des DLT mis en place par la fondation Linux. L'un des projets les plus avancés est Fabric. Conçu comme une base pour le développement d'applications ou de solutions avec une architecture modulaire, Hyperledger Fabric permet d'utiliser des composants tels que les services de consensus et d'adhésion, en plug-and-play. C'est la solution technologique retenue sur le projet We.Trade, une plateforme de Trade Finance gérée par un consortium de banques européennes.

RIPPLE

Ripple est un système de règlement brut en temps réel (RBTR), un marché des changes et un réseau d'envois de fonds par la société Ripple.

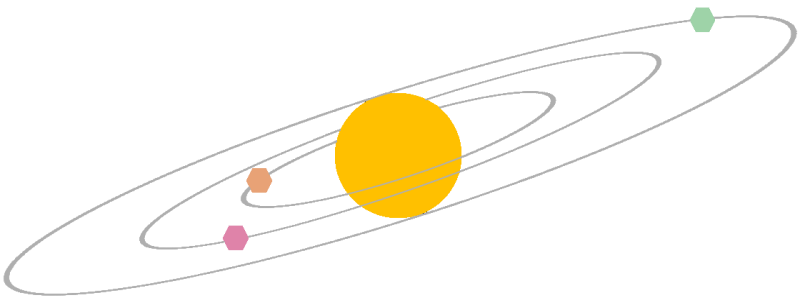
Aussi appelé le Ripple Transaction Protocol (RTXP) ou protocole Ripple3, il est construit sur un protocole Internet distribué et open source, un registre de consensus et une monnaie native appelée XRP (ripples).

STRATUMN

Stratumn est une plateforme française qui propose des solutions autour de la Blockchain. La jeune société ambitionne de garantir fiabilité, traçabilité et intégrité à ses clients. Plusieurs de ces derniers sont d'ailleurs de grands groupes : CNP Assurances, Allianz France, Nasdaq, Thales, Bureau Veritas ou encore Bouygues Immobilier. Elle constitue à ce jour la société française la plus évoluée dans l'utilisation de la Blockchain.

CORDA

Corda est une implémentation de DLT développée par le consortium R3 et n'est pas basé sur la technologie Blockchain. Les transactions ne sont pas rassemblées au sein d'un bloc afin de diffuser les transactions plus rapidement aux membres du réseau. Corda utilise la communication directe entre acteurs et ne diffuse pas largement à tout le réseau. Les transactions sont donc envoyées directement aux parties concernées. Cependant, comme ces transactions ne sont pas publiées sur tout le réseau, aucune entité ne possède l'historique de l'ensemble des transactions qui ont eu lieu sur le réseau. Corda fait apparaître la notion de notaire, qui connaissent l'historique d'une partie du réseau et qui vont valider des transactions sur un périmètre délimité. Corda est pensé comme une couche technologique verticale notamment centrée sur l'industrie financière ; elle intègre un ensemble de fonctionnalités techniques et métiers propres à ce secteur. C'est la solution technologique retenue sur le projet Marco Polo, une plateforme de Trade Finance gérée par un consortium de banques européennes.



Conclusion

A travers cette publication, nous avons souhaité apporter un éclairage sur le fonctionnement et les perspectives de cette technologie. Au-delà du Bitcoin et des fantasmes qui lui sont associés, nous avons cherché à rester factuel et lucide sur le véritable impact de la Blockchain en apportant des éléments de réflexion à nos lecteurs.

A ce stade, nous sommes conscients que cette technologie est encore jeune, complexe et reste limitée à certaines communautés ou à certains secteurs.
Elle devra lever plusieurs contraintes avant d'envisager un déploiement industriel (techniques, organisationnelles, juridiques ou encore éthiques).

Pour autant, on se rend bien compte que la **Blockchain a une portée globale, qu'elle est capable de faire fonctionner des écosystèmes privés ou publics de manière quasi autonome, uniquement sur la base d'algorithmes informatiques**. Potentiellement, elle peut ainsi remettre en cause le rôle de certains agents de confiance qui sont à la base du fonctionnement de nos sociétés actuelles.

Le processus d'appropriation de cette technologie est d'ores et déjà enclenché. Si son potentiel de désintermédiation a pu inquiéter dans un premier temps, l'ensemble des acteurs a désormais saisi l'**opportunité de simplification et de digitalisation des traitements : réduction des coûts et possibilité de créer de nouveaux services à valeur ajoutée**.

Il faut bel et bien considérer la Blockchain comme l'une des composantes de cette nouvelle révolution industrielle qui aura un impact de **transformation des moyens de production, de management et de gouvernance**.

Le déploiement de cette technologie dans l'industrie financière va s'accélérer dans les prochaines années (émergence de nouveaux services, de nouveaux modèles et de nouveaux types de crypto-actifs, adaptation de l'organisation et des processus, premiers retours sur investissement...) jusqu'à un niveau de maturité estimé dès 2025. La Blockchain devrait alors faire partie des technologies dominantes et être pleinement adoptée par les principaux acteurs, notamment en France.

Avec sa volonté de placer Paris en première ligne de l'innovation financière en Europe, le gouvernement se pose en effet en précurseur dans ce domaine, en termes de législation et de cadre de développement. Persuadés du potentiel de la Place de Paris dans le développement de cette technologie, nous comptons nous inscrire dans cette dynamique et poursuivre nos travaux au-delà de cette première publication. Nous souhaitons en particulier analyser plus précisément les impacts de la Blockchain dans chacun des grands métiers de la Finance : corporate finance, activités de marché (gestion d'actifs, dépositaire / tenue de compte de titres), assurance...

La Blockchain n'a donc pas fini de faire parler d'elle...

Contacts
Offre Digital Transformation

R. Teuscher
Partner - Directeur Général
rteuscher@capteo.com

R. Pensec
Directeur
rpensec@capteo.com

Y. Fasla
Senior Manager
yfasla@capteo.com

T. Kucelj
Senior Manager
tkucelj@capteo.com

À PROPOS DE CAPTEO

CAPTEO est un cabinet de conseil en Stratégie, en Organisation et Management, dédié à l'industrie financière et aux marchés financiers. Cabinet de référence dans le secteur financier, nous accompagnons nos clients depuis plus de 12 ans dans leurs réflexions stratégiques, dans la mise en œuvre de leurs projets de transformation et l'amélioration de leurs performances.

Notre sphère d'influence et nos expertises métier se développent autour de 4 segments :
- Les Banques de Financement et d'Investissement
- Les Gérants d'Actifs et les Banques Privées
- Les Services dédiés aux investisseurs
- Les Compagnies d'Assurance, Mutuelles et Organismes de Protection Sociale

Grâce à un accompagnement sur mesure, nos offres de conseil permettent de répondre aux principaux enjeux du secteur financier :
- Définir et mettre en œuvre des stratégies de croissance
- Améliorer la performance opérationnelle et le coefficient d'exploitation
- Conduire les projets de transformation complexes et transversaux
- Gérer les risques et la liquidité des établissements financiers
- S'adapter aux évolutions règlementaires
- Manager la connaissance et le Capital Humain
- Maitriser les données et conduire la transformation Digitale

CAPTEO apporte également son expérience et sa vision de l'évolution du secteur financier en réalisant des études et des benchmarks pour le compte de ses clients.

11 Avenue de l'Opéra, 75 001 PARIS
www.capteo.com