Memo du déjeuner conversation du 10 avril 2019

Thème : **« Blockchain ».** Technologie qui permet d'échanger de la valeur de « pair à pair » sans intermédiaires.

« La blockchain est à la mode. Et si ce nom ne vous dit rien, vous avez sûrement déjà entendu parler de Bitcoin. Dans ce cas, c'est simple : la blockchain est la technologie sous-jacente à Bitcoin. Les experts prétendent que la blockchain va révolutionner notre société autant que l'Internet en son temps. Mais qu'est-ce que c'est vraiment, et comment peut-on l'utiliser concrètement pour développer, aujourd'hui, des applications ? » François Zaninotto (marmelab – 2016) [1]

La blockchain est un nouvel écosystème fait d'algorithmes pour cryptographier et fournir des preuves formelles visant à développer des programmes sans bug. Mais cette technologie pourrait s'insinuer très vite dans de nombreuses applications (banque, santé, industrie, ...).

Une situation qui pose encore une fois la question de la dépendance aux intelligences artificielles et aussi celle de la liberté des individus.

Plus : La blockchain expliquée à ma grand-mère [2]

Définitions :

Blockchain : technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle (*définition de Blockchain France*) [3]

Une blockchain est un **registre** de **faits**, répliqué sur plusieurs ordinateurs reliés entre eux par un réseau pair à pair. On appelle les ordinateurs du réseau des **noeuds**. La communication entre les noeuds est cryptée et garantit l'identité de l'expéditeur et du destinataire. Quand un noeud veut ajouter un nouveau fait au registre, il le propose au réseau qui forme un consensus pour déterminer où (et surtout quand) ce fait doit être inscrit dans le registre. Ce consensus est appelé un **bloc**. (Marmelab).

Petit lexique de la blockchain

Ordre des faits : C'est un algorithme de consensus qui ordonne les faits (données) et crée l'intégrité référentielle de la chaîne.

Blocs : les faits sont regroupés dans des blocs, ils sont ordonnés dans une seule et unique chaîne, qui est répliquée à travers tout le réseau. Chaque bloc pointe sur le bloc précédent. Chaque seconde, chaque noeud mineur au sein d'une blockchain teste des milliers de séquences aléatoires afin d'essayer de former un nouveau bloc.

Cryptographie : c'est un ensemble de procédés visant à protéger (codifier) des informations pour en assurer la confidentialité entre l'émetteur et le destinataire.

Minage : opération technique qui permet de valider un ensemble de transactions à l'intérieur d'un bloc. Les « mineurs », sont les personnes qui gèrent les transactions de la blockchain.

Les contrats intelligents (smart contracts) : Un contrat est une promesse que les parties signataires acceptent de rendre juridiquement exécutoire. Un contrat intelligent peut être défini de la même manière, à la différence que le terme "techniquement" remplace le terme "juridiquement". Plus besoin d'un juge, ou d'une quelconque autorité reconnue par les deux parties, pour valider un contrat.

Quelques généralités :

Enjeux : Si la blockchain sert à échanger de la valeur sans intermédiaire de manière sécurisée, Claire Balva explique les enjeux de la blockchain et en quoi elle a le potentiel de changer de manière structurelle nos rapports en société. Qu'il s'agisse de notre relation aux institutions, banques ou autres tiers de confiance, … La blockchain est beaucoup plus qu'une technologie. C'est un changement radical de paradigme qui est proposé, mettant au centre la confiance comme principe inaliénable.
https://youtu.be/JID9c-MABis (video 13 mn)

➔ Mode de fonctionnement :

Technologie récente (apparue en 2008), elle a été introduite par un inconnu se présentant sous le pseudonyme de Satoshi Nakamoto.

Principe innovant : la solution fonctionne sans organe central de contrôle. Chaque utilisateur peut, à tout moment, à l'aide d'un système cryptographique, vérifier la validité des informations, rajouter des données et enregistrer une transaction.

Lorsqu'un utilisateur effectue une transaction à travers un réseau blockchain, cette dernière est regroupée avec d'autres transactions connexes au sein d'un bloc. Elle est ensuite vérifiée et validée par des membres du réseau à l'aide des techniques cryptographiques. Cette étape dénommée minage, permet d'en vérifier l'authenticité, de s'assurer que sa structure est correcte et qu'elle est cohérente par rapport à celles antérieures déjà enregistrées.

Une fois validé, le bloc est immédiatement horodaté et ajouté à la blockchain. L'opération devient alors visible et accessible à tous les utilisateurs, mais ne peut plus être modifiée, même en cas d'erreur. La rectification nécessite le rajout d'une nouvelle transaction.

La validation d'une transaction est presque instantanée. Elle varie toutefois selon l'importance de l'opération effectuée. Plus [4]

➔ Un nouveau cadre de confiance :

La blockchain met-elle en danger les tiers de confiance ? Partagée par l'ensemble de ses utilisateurs et sans aucun mécanisme central de gestion la blockchain est un système qui vit en autonomie. L'Etat s'y intéresse, tandis qu'à l'étranger, les cas d'usage se multiplient. Au niveau international, un travail de normalisation est en cours. [5]

La blockchain doit trouver sa place dans le système d'information, en articulation avec les processus métier. De multiples usages peuvent s'appuyer sur la blockchain. Ce qui se traduit par une grande diversité de sociétés proposant conseils et développement.

En France la CNIL s'intéresse au sujet. Le Règlement Général sur la Récupération des Données (RGPD) pose question. [6]

➔ Les crypto monnaies :

En 1998, Wei Dai a publié une description de « b-money », un système électronique de trésorerie anonyme.

L'apparition du Bitcoin en 2009, crypto monnaie reposant sur la technologie blockchain, a fait réver plus d'un investisseur. Mais les hauts et les bas des cours, jusqu'à l'effondrement de sa valeur, ont fait déchanter les plus spéculateurs.

Aujourd'hui plusieurs dizaines de crypto monnaies donnent lieu à cotation [7]

Deux visions pour une arnaque ? Après une chute vertigineuse de sa valeur le Bitcoin a perdu de sa superbe, le scepticisme grandit autour des nouvelles devises reposant sur la blockchain.

L'hebdomadaire «The Economist» met en doute l'intérêt de la blockchain, une technologie dont la crédibilité a été mise à mal par la chute du Bitcoin et des autres crypto-monnaies. Énergivores, peu utilisées par le grand public, trop lentes pour être déployées à grande échelle, ces devises d'un nouveau genre relèvent-elles de l'arnaque?

Elles ont pourtant un bel avenir devant elles, a défendu l'économiste Philippe Dessertine lors du Big Bang Éco du Figaro (début 2019). Et si c'était la politique monétaire des banques centrales et a fortiori les monnaies comme l'euro ou le dollar, qui relevaient de l'arnaque? «Comment expliquer les taux négatifs? Comment justifier que la dette mondiale atteint 240.000 milliards de dollars alors que le PIB mondial, lui, s'élève à 90.000 milliards de dollars?» Questionne le directeur de l'Institut de haute finance. Convaincu que la prochaine crise financière proviendra de l'excès d'endettement public, avec le risque d'une perte de confiance dans les monnaies «traditionnelles». Place libre aux crypto monnaies !?

A terme, les crypto-devises comme le Bitcoin ou l'Ether pourraient constituer une alternative alléchante. Forts de leur puissance financière et de leur emprise mondiale, les géants du web voient venir le coup et envisagent d'émettre leur propre crypto-monnaie. Le Facebook Coin, censé sortir à l'été 2019, pourrait ainsi concurrencer un jour l'euro ou le dollar. Apple et Amazon devraient suivre.

À l'image du très célèbre Bitcoin, Ethereum est un autre système, générant une crypto monnaie, qui repose sur la technologie Blockchain. Néanmoins, les similitudes avec le mastodonte de la monnaie virtuelle s'arrêtent là, car Ethereum est une Blockchain Open Source. Cela signifie que son code informatique est ouvert à tous, permettant à n'importe qui de développer des services et applications sur la plateforme Ethereum.

Rappel : Alors que 53% de la population n'ont pas de compte bancaire dans le monde, le 7 avril 2019 17.630.000 bitcoins en circulation. Cours et volume des transactions [8]

➔ La blockchain pour quoi faire ?

Finalement la blockchain quel qu'en soit sa forme est devenue le sujet à la mode dans le microcosme des experts du digital. Si tout le monde cherche à comprendre de quoi il s'agit, beaucoup sont convaincus qu'il s'agit d'une technologie révolutionnaire.

Plusieurs secteurs d'activités se lancent dans des exploitations pour améliorer leurs services (ou leurs performances) sous forme de « contrats intelligents » (pas dépendant d'un tiers).

Parmi ces réalisations on trouve :
- un moteur de recherche d'images conçu pour attribuer correctement les photos à leurs auteurs. Développé par Mediachain ;
- des projets pour gérer les droits d'auteurs sont actuellement à l'étude. L'artiste est le dernier a être payé. Avec la blochain les artistes pourraient reprendre le contrôle de leurs droits.
- dans l'immobilier, des start-ups proposent des services liés au stockage et à la transmission de l'information décentralisée aux professionnels du secteur. Parmi elles : Olarchy, Keeex.me et MyNotary, par exemple, qui permettent de déposer les documents liés à une vente sur la blockchain : mandat, dossier technique amiante, offre d'achat… Chaque document a sa propre empreinte digitale, assurant son authenticité. Ils sont consultables à tout moment par les parties concernées et constituent un historique de l'état du bien. Dans la même veine, Bitproof permet de certifier des documents. L'intérêt de tels services réside dans la transparence des informations, l'égalité entre les différents acteurs, la sécurisation et l'authenticité des données. Ils peuvent s'avérer particulièrement utiles dans les premières étapes de diagnostics. « *Pour la transaction en tant que telle, il y a toujours un notaire. La plateforme ne remplace pas un officier de l'Etat ; c'est bien le notaire qui signe l'acte authentique* », prévient Michael Sigda, co-fondateur d'Olarchy.

Aux Etats-Unis ou en Suède, des start-ups comme Ubitquity ou Chromaway travaillent sur des prototypes de registre foncier basés sur la blockchain. Au Ghana, l'ONG Bitand a lancé une application avec la blockchain pour établir un cadastre. En Géorgie, le gouvernement a lancé un partenariat avec l'entreprise BitFury pour digitaliser le cadastre.

Dans d'autres domaines aussi la blockchain semble proposer des solutions :
- tracabilité dans la chaîne alimentaire ;
- pour lutter contre la sécheresse en Californie une régulation de la distribution d'eau dans l'agriculture a été mise en place ;
- dans le domaine du transport maritime, la même démarche de co-création entre Maersk et IBM a donné l'impulsion à la plateforme TradeLens, qui regroupe des informations précises sur le cycle de vie des marchandises transportées (identité des différents transporteurs, tampons de douane). Ce partage de documents dématérialisé améliore l'efficacité des opérations de transport, qui utilisent aujourd'hui beaucoup de papier. Compte tenu du volume de marchandises qui utilise le transport maritime, l'économie réalisée se mesure en milliards de dollars.

D'autres solutions sont en phase d'exploration dans la pharmacie, la cosmétique ou encore le luxe, notamment sur des questions de contrefaçon.

Pour EDF la blockchain remplacera les garanties d'origine pour la production et la consommation d'énergie « verte ». [9]

Les grandes écoles dans la perspective blockchain. Le 4 avril 2019, Capgemini, l'École polytechnique et sa Fondation lancent une chaire dédiée aux implications technologiques et économiques de la blockchain afin de promouvoir l'enseignement supérieur et la recherche dans ce domaine émergent.

Fantasmes et espoirs : Gartner estime dans son CIO Survey que la valeur de la blockchain dépassera les 310 milliards d'euros à l'horizon 2026, avant d'exploser à 2 700 milliards d'euros d'ici 2030. Autant dire que les DSI ont tout intérêt à s'emparer de ce sujet afin que leur organisation anticipe cette révolution technologique et reste ainsi concurrentielle. The reality of blockchain [10]

➔ Qui gère la blockchain ?

Blockchain publique versus blockchain privée et de consortium. Lorsqu'on parle de blockchain, on parle aussi souvent de 3 principes qui s'opposent, la blockchain publique, celles de consortium et les blockchains privées. Techniquement, il s'agit toujours de la même technologie, dans un cas celle-ci est utilisée sur un modèle totalement décentralisé et ouvert, celui de la version publique (Bitcoin ou

Ethereum), dans l'autre cas, celui de la blockchain de consortium ou privée, le modèle est partiellement ou totalement fermé. Les différences sont nombreuses et portent sur des aspects fondamentaux de la blockchain, lorsqu'elle est publique, les utilisateurs sont totalement anonymes, la validation des transactions est ouverte à tous, les données qui transitent sont visibles de tous. Dans le cadre de la blockchain privée ou de consortium, les utilisateurs sont connus et c'est d'ailleurs ce qu'ils recherchent, le mode de validation est quant à lui répartit entre les acteurs du consortium ou bien centralisé et maîtrisé par un seul acteur pour la version privée. Vous l'aurez compris, en fonction du mode de fonctionnement, chacune de ces versions de la blockchain a des applications totalement différentes.

➔ De nouvelles questions éthiques ?

Absence d'un cadre réglementaire. Le déploiement de la blockchain dans les différents secteurs semble encore en être à ses premiers balbutiements. Sur le plan technique, tout est possible pour que cette technologie soit pleinement exploitée. Néanmoins, l'absence de cadre réglementaire et de normes internationales destinés à cerner le déploiement de cette technologie constituent des obstacles majeurs.

Ce besoin est d'autant plus important que le procédé de chaîne des blocs pose un problème d'éthique : l'accès aux données personnelles des particuliers (en cas d'intrusion).

Les limites en matière de sécurité. Malgré toutes ses promesses, la blockchain présente des limites en matière de sécurité. Une cyber-attaque massive du réseau serait lourde de conséquences.

Même si ses promoteurs affirment que le système ouvert de la blockchain n'est pas synonyme de système non sécurisé. La technologie utilisée est protégée contre la falsification ou la modification par des nœuds de stockage. Ces derniers forment une chaîne de blocs de données invariables, d'où la nomination.

Le rajout de nouvelles transactions n'est possible qu'après la validation de plusieurs participants du réseau appelés « nœuds du réseau ». Ces derniers emploient leurs unités de calcul (algorithmes) pour vérifier l'authenticité de l'opération en la comparant avec les opérations précédentes, identifiant sa traçabilité et examinant les transactions connexes. Il devient ainsi difficile pour les hackers de simuler ou de manipuler des blocks d'information interconnectés.

Sur le principe, cette transparence et cette inaltérabilité permettent aux utilisateurs d'effectuer des transactions en toute confiance, même en l'absence d'une autorité centrale.

En juin 2018 une attaque 51% [(11)] de ZenCash a entraîné une perte de 558 000 euros. Une attaque sur Bitcoin Gold, en mai de la même année a fait perdre à la crypto monnaie plus de 18 millions de dollars. En fait, 2018 était l'une des pires années d'attaque par blockchain de l'histoire. Ces attaques sont une arme à double tranchant, car à mesure que le public est informé d'une attaque, la crypto-monnaie ciblée devient mentalement dévalorisée. Et ces situations mettent a mal la promesse de sécurité et de fiabilité de la technologie blockchain.

Et l'humain. Avec des technologies toujours plus complexes, des appareillages disparates et des accès à l'internet parfois difficile (zones blanches) comment envisager qu'une nouvelle solution technologique soit bonne pour tous ? Il y aura toujours ceux qui avancent avec les évolutions proposées et ceux qui sont laissés sur le bord du chemin. Et l'écart croît inexorablement.

➔ Combien ça coûte ? Qui paye ?

Gratuit ou presque ! La force de la blockchain est donc de permettre de se passer des intermédiaires qui prennent leurs commissions pour réaliser des transferts d'argent ou de documents. Finalement, seul les mineurs gagnent de l'argent dans le système et ce quel que soit le montant des transactions que contient le bloc validé. Et pour les utilisateurs de la blockchain, c'est tout bénéfice. Ainsi dans un système traditionnel dans lequel vous souhaitez transférer de l'argent, l'intermédiaire va prendre une commission pour la réalisation de cette transaction, le montant de cette commission est généralement fonction du montant transféré, donc plus vous transférez d'argent plus vous êtes ponctionnés. Dans la blockchain, le transfert d'argent coûte quelques centimes seulement et ne dépend aucunement du montant des sommes transférées, ce modèle est donc plus intéressant pour les utilisateurs.

Une forte consommation d'énergie pour une technologie énergivore. Les analystes les plus écologiques s'inquiètent. Ils ne partagent pas l'enthousiasme de certains de leurs confrères. Cette technologie nécessite une forte consommation d'énergie.

Selon les chercheurs de l'Institut Mines-Télécom (IMT), la généralisation de l'activité de minage de la blockchain, nécessiterait une consommation d'énergie égale à 100 fois la puissance utilisée

aujourd'hui par l'ensemble des serveurs de Google.
Autre indicateur, pour bien fonctionner, si l'utilisation de la blockchain se généralise elle aura besoin d'une énergie égale à huit fois la consommation française actuelle. Cette situation va poser problème.

➔ Sous forme de conclusion

La technologie blockchain est à la fois mystérieuse et excitante. Est-ce qu'elle pourrait aboutir à cette révolution prédite? Ou est-ce juste une bulle spéculative construite sur une idée bancale ? La question reste posée. Mais à voir comment les groupes les plus puissants de l'économie mondiale fourbissent leurs projets avec cette technologie nous pouvons nous attendre à subir de nombreuses applications à base de blockchain.

« À ce stade, la blockchain a le potentiel d'aller dans deux directions très opposées. La crédibilité subjective des réseaux pourrait déboucher sur une plate-forme éthique, décentralisée et fiable, …, permettant à l'humanité d'avoir accès à une identité numérique sûre et privée et de confier le pouvoir d'Internet à la population. Ou bien, la nature immuable des réseaux et le manque de gouvernabilité pourraient conduire à une utilisation abusive généralisée et à une vulnérabilité systémique… …Guidés par l'éducation et la sensibilisation, travaillons ensemble pour utiliser la blockchain pour son incroyable potentiel, tout en corrigeant certaines des conséquences inattendues d'une innovation rapide. » (Nicolas, https://news-investissement.com)

Restons vigilants et informés !

Sources et renvois :
Compilations d'extraits du web et de lectures.

(1) **Marmelab, atelier d'innovation digitale :** https://marmelab.com/fr/
(2) **La blockchain expliquée à ma grand-mère :** https://indeed.headlink-partners.com/2019/01/31/blockchain-et-asset-management-part-1-la-blockchain-comme-expliquee-a-ma-grand-mere/
(3) **Blockchain France :** https://blockchainfrance.net/
(4) **Fonctionnement de la blockchain :** https://www.blockchain-info.fr/
(5) **Normalisation de la blockchain :** https://normalisation.afnor.org/actualites/bientot-normes-iso-blockchain/
(6) **RGPD et blockchain :** https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf
(7) **Cotation crypto monnaies :** https://www.abcbourse.com/marches/cryptomonnaies.aspx
(8) **Cours et transactions du Bitcoin :** https://bitcoin.fr/le-cours-du-bitcoin/
(9) **EDF et blockchain :** https://www.edf.fr/collectivites/le-mag/le-mag-collectivites/decryptage-du-marche-de-l-energie/la-blockchain-remplacera-les-garanties-d-origine
(10) **Gartner, The Reality of Blockchain :** https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/
(11) **Les attaques 51% :** https://journalducoin.com/bitcoin/bitcoin-gold-btg-fail-186-millions-de-dollars-pirates/

Et aussi :
Imaginer Demain : https://www.imaginer-demain.fr/?s=blockchain
Utiliser blockchain, 8 exemples concrets : https://www.archimag.com/demat-cloud/2018/10/29/comment-utiliser-blockchain-8-exemples-concrets
Applications Blockchain : https://www.usine-digitale.fr/blockchain/
Tout sur le Bitcoin : https://bitcoin.fr/faq/
Sur Wikipedia : https://fr.wikipedia.org/wiki/Blockchain
Crypto monnaies, le piège de la caricature : https://www.lepoint.fr/high-tech-internet/cryptomonnaies-le-piege-de-la-caricature-09-02-2018-2193672_47.php
Les intermédiaires derrière la blockchain : https://atelier.bnpparibas/prospective/article/intermediaires-cachent-derriere-blockchain
Un bouleversement économique, juridique, sociétal, … : https://www.cairn.info/revue-i2d-information-donnees-et-documents-2017-3-page-20.htm?try_download=1#
Les PME françaises et la blockchain : https://www.lesechos.fr/finance-marches/banque-assurances/les-pme-tricolores-se-branchent-sur-la-blockchain-1007561
Video de vugarisation (34 mn) : https://www.youtube.com/watch?v=SccvFbyDaUI