DOSSIER

Une nouvelle technologie : la Blockchain

Bernard Soret (75 ILI) et Jean-Marie Heyberger (74 ILI), membres du Comité de rédaction

Après la révolution internet au niveau de l'information, la blockchain va rentrer dans notre quotidien. Notre Dossier lui est consacré, car nous souhaitons être au cœur des changements, à travers nos dossiers.
Chaque seconde, les entreprises échangent de la valeur avec des fournisseurs, des partenaires, des clients et autres tiers. Par valeur, nous entendons les biens, les services, l'argent, les données. Ces échanges sont, aujourd'hui, réalisés avec ou sans tiers de confiance et manquent parfois d'efficience, de fiabilité. Un processus effectué souvent via un intermédiaire et qui peut s'avérer lent, coûteux et corruptible.
Chaque échange de valeur est une transaction. Les transactions réussies doivent être rapides, précises et facilement acceptées par les parties prenantes.
La Blockchain se définit comme une technologie de stockage et de transmission de l'information, sans organes de contrôle, et donc transparente, sécurisée et décentralisée. Elle facilite aux entreprises l'exécution rapide, fiable et transparente de leurs transactions. Elle permet la désintermédiation en étant elle-même un tiers de confiance dématérialisé, distribué, rapide et transparent. Les transactions seront validées et enregistrées.
Les premiers grands secteurs d'utilisation sont la banque, l'assurance, la logistique, l'énergie, la santé, l'aéronautique, l'immobilier, l'économie collaborative…
Nos alumni et quelques experts interrogés sur cette technologie prometteuse nous partagent leurs compétences, leurs expériences, leurs attentes et parfois leurs réticences. Nous pourrons, ainsi, mieux maîtriser les enjeux et les risques.

QU'EST-CE QU'UNE BLOCKCHAIN ?

C'est un enchaînement de blocs - un bloc étant une sorte de container de données numériques.
Chaque bloc est identifié par un code cryptographique : le hash.
Les blocs s'enchaînent les uns après les autres pour former la chaîne de blocs, en respectant 2 critères :

- *Un nouveau bloc ne peut s'enchaîner au dernier bloc de la chaine que si son hash est compatible avec le hash précédent, à la manière de deux pièces de lego qui s'emboîtent.*
- *L'ordre d'enchaînement est chronologique.*

Dynamique sociale de la blockchain

Etienne Perrot, jésuite, professeur d'économie et d'éthique (Paris, Fribourg)

La blockchain ouvre-t-elle une ère nouvelle ? Politiquement, peut-être. Culturellement non, car elle incarne simplement un aspect de l'idéologie du capitalisme actuel. La blockhain porte, en effet, trois valeurs, indispensables au bon fonctionnement du marché libéral : la sécurité des échanges, l'autonomie individuelle appuyée sur le secret, l'efficience économique.

Pour parler français, une «chaîne de blocs» est une opération de cryptographie, inscrite dans un réseau électronique, sans organe central de contrôle, et qui retient d'une manière indélébile l'historique de tous les échanges de contrats, images, signes monétaires, signatures, caractéristiques fondamentales d'un produit… etc. On parle de «blocs» parce que les messages cryptés sont transcrits par groupes successifs dans le système. On parle de «chaîne» parce que la cryptographie de chacun de ces blocs inclut la cryptographie du bloc précédent.

La sécurité des échanges

Au service des marchés, la blockchain est typique de la science d'aujourd'hui qui solutionne les problèmes par des moyens approchés, de plus en plus performants, sans jamais toucher la perfection. En effet, la cryptographie asymétrique d'aujourd'hui ne relève pas du seul génie mécanique ; elle convoque également la puissance de calcul des computers. Loin des «codes secrets» connus dès la plus haute antiquité, l'actuelle cryptographie est fondée sur des fonctions mathématiques dites de hashage (en français, hachage). Ces fonctions dites asymétriques font irrésistiblement penser à la viande hachée à partir de laquelle il est bien difficile de retrouver la texture du filet de bœuf, sauf par recombinaison

de tous les morceaux, par essais et erreurs, ce qui sollicite une énorme puissance de calcul.

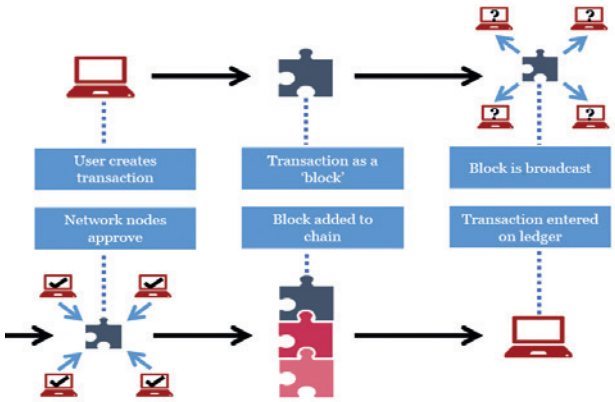
Parmi ces fonctions asymétriques, les meilleures possèdent trois qualités. D'abord, elles sont telles que la moindre modification du message initial (de longueur indéfinie) produit une très différente empreinte (qui est sa traduction dans un nombre fini d'éléments, à la manière d'un cryptogramme) ; ce qui permet de vérifier facilement l'intégrité du message initial. Ensuite, elles interdisent de remonter facilement du hachis au message initial. On dit qu'elles «résistent à la pré-image». Enfin, elles ne permettent pas la traduction par une même empreinte de plusieurs messages différents, elles «résistent aux collisions».

Aucune fonction de hachage n'obéit parfaitement à ces trois injonctions. Pour la pratique, il suffit que soit disproportionné le temps de calcul pour découvrir le message initial correspondant à l'empreinte, compte-tenu de la puissance des computers disponibles. La sécurité, ici conçue comme l'adéquation du message et de son empreinte, n'est jamais garantie pour l'avenir ; c'est une sorte de course-poursuite entre mathématiciens et puissance de calcul, pour l'instant largement gagnée par les mathématiciens.

Le secret au service de l'autonomie individuelle

La cryptographie électronique a intéressé, outre les Services secrets, les Cypherpunks (sic) (littéralement, les anarchistes du chiffrage) dès les années 1980, au moment où le système Internet laissait entrevoir le danger d'un contrôle de la vie privée par une administration publique tentaculaire. La blockchain pousse ainsi à l'extrême la tendance culturelle du «do it yourself» (littéralement faites-le par vous-même), mais en dehors des plateformes administratives ou commerciales, dont le projet de monnaie privée, Libra initié par Facebook est l'un des avatars, qui font travailler gratuitement les assujettis et les clients. Par la blockchain, on dévalorise l'instance politique en échappant aux normes édictées par le coordinateur central. Un pas essentiel a été franchi lorsque, à la fin des années 1990, fut découvert le moyen de remplacer l'intermédiaire de confiance par un contrôle multipolaire réparti sur le web. Car, dans les transferts électroniques, la plus grande menace qui pèse sur le secret est l'usurpation d'identité ou, à l'inverse, son dévoilement, particulièrement facile dès lors que l'on a accès au fichier central chargé des interconnections entre partenaires. Ainsi en fut-il pour les comptes cachés dans les paradis fiscaux. Avec la blockchain, pas de fichier central, pas d'intermédiaire qui contrôle l'identité des partenaires, la légalité de l'opération et la bonne fin du transfert.

C'est la raison pour laquelle la première application de cette technologie électronique qui associe identités cryptées et visibilité publique de toutes les transactions fut la création du bitcoin, une cryptomonnaie née en 2009, qui, depuis, a montré, pour des usages parfois discutables, la robustesse du système.



L'économie des frais d'intermédiation

En négatif, pour l'économie comme pour l'écologie, la puissance de calcul mobilisée par les blockchains consomme une énorme quantité d'énergie électrique, sans parler des coûts du matériel utilisé, de la rémunération des techniciens de maintenance, des informaticiens qui élaborent les algorithmes de hachage et des mathématiciens qui mettent au point les fonctions asymétriques. Le tout est à comparer, bien sûr, avec les avantages attendus. Des progrès sont encore possibles. Toujours dans le sens de l'économie, il y a des blockchains dites «de consortium» réservées à quelques participants (par exemple un groupe d'institutions financières) qui se réservent le droit de modifier, sur décision majoritaire, les protocoles d'accès ou de fonctionnement de la blockchain. Il existe enfin des blockchains dites «privées» propres à une organisation, ou à une entreprise. Dans ce cas, la blockchain n'a évidemment pas besoin d'être aussi performante en termes de sécurité, ce qui économise beaucoup de temps et d'énergie.

Bref, la source principale de l'efficience économique de la blockchain est l'absence d'un intermédiaire qu'il faudrait rémunérer. Ce qui ouvre à la blockchain une carrière d'usages très diversifiés : paiements internationaux en convertissant les monnaies officielles en crypto-monnaies pour les faire transiter avant de les reconvertir à l'arrivée ; transfert et stockage sécurisé de valeurs mobilières, de titres de propriété, rendant à terme inutiles autant les notaires que les plateformes électroniques d'économie partagée, genre Uber ; contrôle des processus de fabrication et de distribution de produits ; sécurisation des procédures électorales là où l'on peut légitimement se méfier des scrutateurs, etc. Les applications les plus prometteuses de la blockchain, grâce aux objets connectés, sont les smart contracts (en français, contrats intelligents) dont la contrepartie se dénoue automatiquement en cas de réalisation de l'occurrence prévue. Par exemple paiement automatique de l'indemnité en cas de retard d'un avion. On rêve qu'il en soit de même pour la SNCF. Là encore, économie de temps et de moyens en perspectives.

L'avenir de la blockchain

Comme Internet sans lequel elle n'existerait pas, la blockchain se développera au rythme du capitalisme libéral, en même temps que l'individualisme contractuel où chacun se sent tenu de ne faire que ce à quoi il s'est engagé par contrat, dans la méfiance de toute interface capable d'interférer avec sa liberté individuelle. Pour faire correspondre cette culture capitaliste avec les valeurs de tradition chrétienne, il conviendrait d'instiller dans la logique contractuelle un plein souci de discernement où le bien commun, le bien de chacun dans la solidarité de tous, remplacerait le seul souci de l'intérêt et du bien-être individuels. Le rapport-au-monde (la spiritualité) qui s'ensuivrait conduirait à inverser la célèbre formule libérale « ma liberté s'arrête là où commence la tienne » qui deviendrait, paradoxalement « ma liberté commence avec la tienne ».

Quoi qu'il en soit de ces jugements moraux et spirituels, j'entrevois pour la blockchain un scénario semblable à celui d'Internet : en même temps que des promesses de démocratie radicale et de libre collaboration universelle, Internet a favorisé assez vite le contrôle bureaucratique d'une part, et d'autre part la domination des GAFAM (qui provoquera sans doute une réaction des États), domination d'autant mieux acceptée qu'elle se pare des valeurs de notre modernité, sécurité et performance.

Une première lecture de la blockchain dans l'industrie pharmaceutique

Philippe Jeanne-Julien (94 INA)

Du consumérisme digital à l'entreprise digitale

Les technologies digitales sont «tendance»… surtout lorsqu'il s'agit de démontrer, ou plutôt de communiquer, la capacité d'innovation de telle ou telle compagnie ; et de s'afficher comme précurseur ou prescripteur dans un domaine d'activité donné. Nous les consommons sans modération. Elles sont le nouvel eldorado de nombre de start-ups, le moyen d'attirer de jeunes talents ; et à en croire certains, le remède à tous les maux.

L'industrie pharmaceutique ne déroge pas à la règle, même si les technologies digitales y sont arrivées plus tardivement. Mais le rythme s'accélère et la frénésie gagne.

A tel point que si nous ne voulons pas succomber aux sirènes des multiples sollicitations et nous perdre dans le «nuage», il est désormais temps de poser le crayon et de définir des priorités. Bref, revenir aux questions si simples mais fondamentales : Pour quoi faire ? Et comment ? Et clarifier ainsi la vision et la stratégie qui nous feront passer du statut de consommateurs digitaux au rang d'entreprise digitale.

La quête du sens et le sens des contraintes…

C'est la démarche engagée – au sein d'un groupe d'innovation basé sur notre site SI bordelais – en regard de l'émergence des initiatives autour de la blockchain.

A l'origine, le principe de blockchain n'est pas simple à appréhender. On en parle beaucoup, ceux qui en parlent n'ont pas nécessairement compris ce dont il s'agissait, et les définitions possibles sont multiples. J'ai, personnellement, fini par en trouver une – elle n'est pas de moi - mais qui donne, à mon sens, les bases nécessaires à l'identification de possibles cas d'emploi.

«La blockchain est une technologie de stockage et de transmission d'informations qui est sécurisée, transparente, et qui fonctionne sans organe central de contrôle». Je ne m'étendrai pas plus sur les détails car, finalement, ce n'est pas tant cette définition qui est importante, que les perspectives qu'elle peut ouvrir; perspectives qui ne doivent pas occulter les contraintes auxquelles il faudra faire face, particulièrement dans le domaine pharmaceutique.

Ainsi, l'un des atouts majeurs de cette technologie, à savoir l'absence d'organe central de contrôle, peut se révéler devenir un écueil incontournable dès lors qu'il s'agit de valider ce type de fonctionnement auprès d'autorités réglementaires souvent conservatrices. L'enjeu majeur est d'établir la confiance. Il s'agit, en effet, de se reposer totalement sur un protocole informatique. Celui-ci garantira l'alignement de tous les acteurs sur l'historique des transactions et informations contenues dans le registre partagé, mais ne sera détenu par aucun d'entre eux. Personne n'a la main sur le registre. Pas facile à faire admettre à des qualiticiens habitués à voir tracer, documenter et valider nominativement la moindre modification de système informatisé. D'autant moins facile, que dans certains cas, cela pourrait remettre profondément en cause, au-delà de leurs méthodes de travail, leur positionnement même dans l'écosystème pharmaceutique. Le tout, sans oublier les origines plus ou moins sulfureuses du développement de ce protocole dont on ne connaît aujourd'hui encore que le pseudonyme de son concepteur en 2008 (Satoshi Nakamoto). D'où l'intérêt d'investiguer plus en profondeur l'intégration des processus de validation requis par les autorités de santé au sein même du protocole.

Passée cette nécessaire adéquation aux exigences pharmaceutiques, les perspectives sont nombreuses et exaltantes. Il y a les plus faciles à identifier: la gestion de chaînes logistiques complexes, par exemple. Surtout, quand les agréments et attributs réglementaires y sont prépondérants, comme c'est le cas dans l'industrie pharmaceutique. Il y a, également, les applications liées à la traçabilité et la sérialisation des médicaments (identification unique garantissant l'absence de contrefaçon au point de dispensation). Mais au-delà, on peut envisager des usages plus poussés. Le partage continu des informations relatives aux différentes phases d'études cliniques - via blockchain - pourrait réduire les temps de mise sur le marché de nouveaux produits… L'horizon est définitivement ouvert !

Et l'Icam dans tout ça ?

Je n'aurais jamais imaginé, durant mes années d'études à l'Icam, travailler un jour dans les systèmes d'information. Je n'en ai perçu les enjeux profonds que plus tard, durant mes années d'exercice en supply chain.

Mais je suis désormais convaincu que l'essor des technologies digitales est un terrain de jeu passionnant. Beaucoup plus que l'informatique de gestion de mes débuts. Des métiers se créent qui sont autant d'opportunités pour de jeunes Icam, que je sais armés pour savoir tout à la fois : bâtir la vision, garder le sens profond des choses, le tout avec la dose d'éthique appropriée.

La blockchain : l'avenir des échanges sur internet ?

Sylvain Michel (118 ATO)

Dans quelle mesure puis-je vous en parler ?

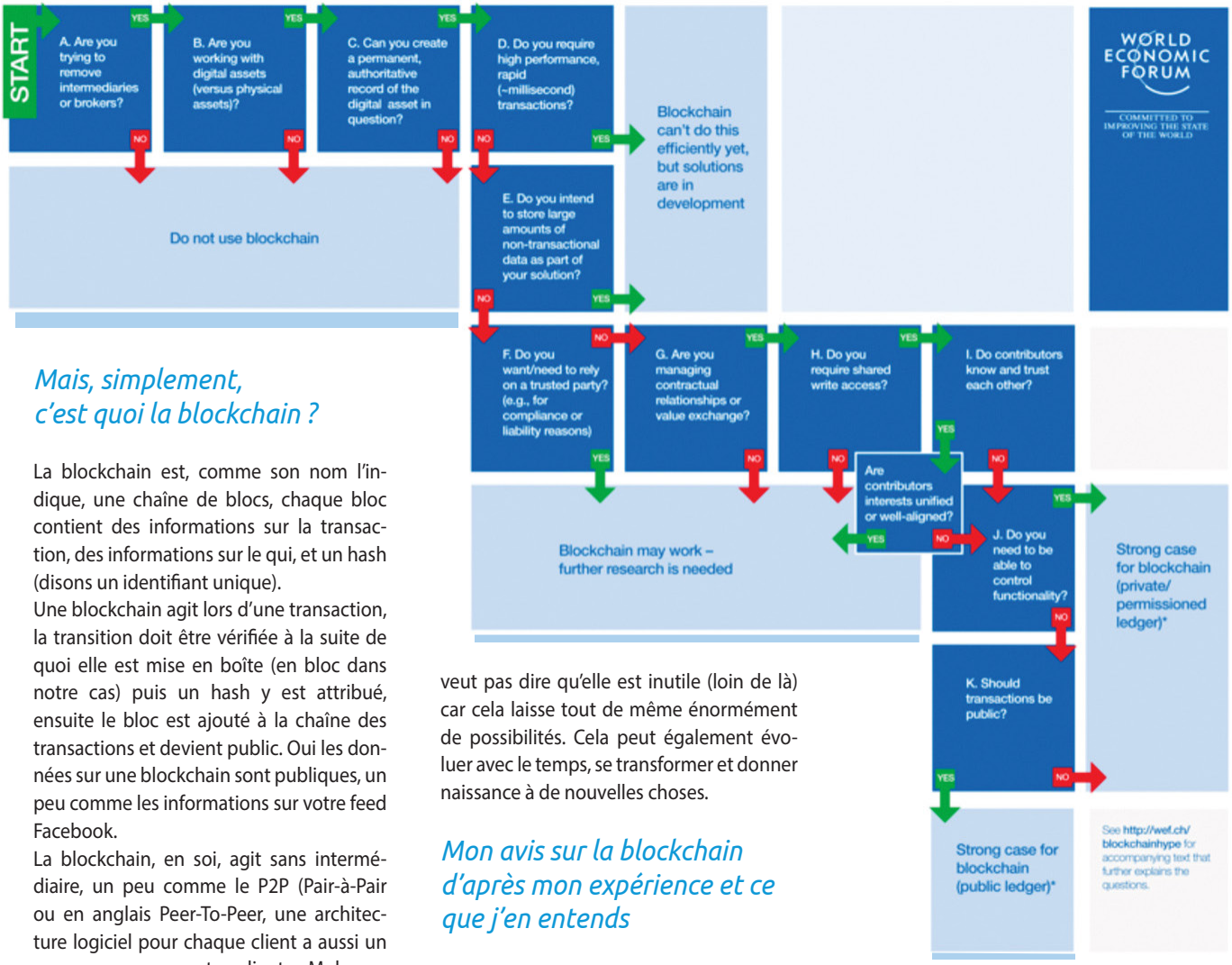
Continuant actuellement mes études sur un M.Sc in computing à l'université polytechnique de Poznań (Pologne), je travaille en même temps en tant que développeur SAP Fiori au département IT Mocny (informatique fort) de Arvato Bertelsmann.
Je ne suis pas un expert de la blockchain, mais c'est une technologie qu'il m'arrive de côtoyer dans ma poursuite d'études ainsi qu'au travail.

Mais, simplement, c'est quoi la blockchain ?

La blockchain est, comme son nom l'indique, une chaîne de blocs, chaque bloc contient des informations sur la transaction, des informations sur le qui, et un hash (disons un identifiant unique).
Une blockchain agit lors d'une transaction, la transition doit être vérifiée à la suite de quoi elle est mise en boîte (en bloc dans notre cas) puis un hash y est attribué, ensuite le bloc est ajouté à la chaîne des transactions et devient public. Oui les données sur une blockchain sont publiques, un peu comme les informations sur votre feed Facebook.
La blockchain, en soi, agit sans intermédiaire, un peu comme le P2P (Pair-à-Pair ou en anglais Peer-To-Peer, une architecture logiciel pour chaque client a aussi un serveur pour un autre client, eMule par exemple est P2P).
Cependant la blockchain permet le transfert de valeurs (entre autres monétaires, comme le montre sa première application historique avec le bitcoin).
Aussi la blockchain est sécurisée et donc, au moins théoriquement, hacker-proof.

Alors la blockchain c'est la baguette magique des échanges de données ?

Spoiler alert : non, la blockchain a même des use cases très précis (du point de vue d'un développeur). Voici l'exemple des 11 questions que j'ai beaucoup vues utilisées pour le choix de la Blockchain ou non :
Ce schéma est fait sur des critères économiques mais peut facilement être adapté à d'autres domaines. Certes, cela limite beaucoup l'utilisation de la blockchain, ce qui ne veut pas dire qu'elle est inutile (loin de là) car cela laisse tout de même énormément de possibilités. Cela peut également évoluer avec le temps, se transformer et donner naissance à de nouvelles choses.



Mon avis sur la blockchain d'après mon expérience et ce que j'en entends

Sur les points suivants, je ne peux pas être objectif car la blockchain reste malgré tout une nouvelle technologie, je vais donc donner davantage un avis ou une pensée.

La blockchain et la sécurité

Pour ma part, je place la blockchain à la même place que la "security by design" appliquée au génie logiciel (c'est-à-dire penser à la sécurité dès la conception et, dès que possible, sécuriser via la conception/ architecture). Oui, c'est sécurisé, car bien davantage que les solutions classiques, mais pas forcément inviolable: tout système informatique actuel a, la plupart du temps, une faille: le fait qu'elle n'est pas encore été détectée ou rendue publique ne veut pas dire qu'elle n'existe pas. A savoir aussi que la plupart des attaques sont du phishing (c'est à dire en récupérant les informations nécessaires à la source : l'utilisateur). La sécurité d'un système n'est pas forcément égale à la sécurité de l'utilisateur, l'erreur humaine est la plus grande faille de sécurité. En développement infor-

matique, on dit souvent de ne jamais faire confiance à l'utilisateur qui peut crasher le système, soit par erreur, soit car il est mal intentionné, or la blockchain repose sur la confiance entre les utilisateurs.
D'un point de vue éthique, il est aussi à savoir que beaucoup de gens sont bien plus mal intentionnés quand ils sont protégés derrière un écran (juste à voir le harcèlement en ligne par exemple).
De plus des protocoles d'échange plus sécurisé sont déjà en développement grâce à la physique quantique, une transmission d'information ou une intrusion est détectée par un changement d'état comme vous pouvez le voir dans le reportage YouTube "The Race For Quantum Supremacy I VICE on HBO" à peu près à 8'10".

La blockchain et les entreprises

Entreprise ouverte et open-source

L'actuelle blockchain se base sur la confiance et la transparence, un peu à la façon des "nouvelles" entreprises ouvertes ou des projets open-source.
Ces entreprises et ces projets pourraient donc tirer parti de la blockchain lorsque leurs cas d'utilisation rejoignent ceux de la blockchain.
Cependant et malheureusement, du moins pour les projets open-source, ils sont souvent bien moins populaires, dans la vie de tous les jours, que ceux propriétaires à performance égale. Par exemple, ici, parmi nos lecteurs, qui utilise Microsoft Office et qui utilise Libreoffice ? Qui a Windows/Apple sans même considérer une distribution Linux (comme Ubuntu ou Mint qui sont tout aussi simples sinon plus, bien plus légers et respectent vos données et votre vie privée davantage que Apple ou Microsoft) ?

La blockchain, selon moi, se heurte aux mêmes risques que les projets open-source actuels : c'est à dire, des utilisations principalement dans des projets open source, des associations, pour quelques utilisateurs avertis/curieux et / ou initiés.

Entreprise conservatrice et propriétaire

Les entreprises plus conservatrices (ou, du moins, moins ouvertes au niveau des données ainsi que les logiciels propriétaires) subissent, quant à elles, le double tranchant de la blockchain qui se retrouve être à la fois une opportunité et une faiblesse.
Par exemple, pour des entreprises comme Uber ou BlaBlaCar, cela remet totalement en cause leurs business model, voire leur raison d'être, en effet la blockchain permettrait un transfert direct entre le conducteur et le passager sans intermédiaire (ici Uber ou BlaBlaCar), cependant, ici, l'intermédiaire est aussi la plateforme du service et, sans cette plateforme, difficile pour le conducteur et le passager de rentrer en contact de la même façon (de plus, le système de confiance instauré par la plateforme n'existerait peut-être pas naturellement entre le passager et le conducteur).
Cependant ; pour beaucoup d'entreprises "non ouvertes" une blockchain moins transparente et publique serait une opportunité (bien que l'on puisse d'ores et déjà un peu tricher sur le côté "publique" en utilisant un nom d'utilisateur ou un identifiant quelconque) mais serait-ce encore une blockchain ?

La blockchain de demain

Pour ma part, je pense que la blockchain a de l'avenir, qu'elle va évoluer et se transformer. Je vois principalement 2 chemins pour la blockchain dans un futur proche. Ces deux chemins sont étroitement liés et pourraient bien se dérouler tous deux et se mélanger.

La blockchain +

Une des voies que j'appellerai la blockchain + est d'utiliser la blockchain en relation avec d'autres technologies (en fait c'est déjà plus ou moins le cas avec les plateformes qui permettent l'accès à une blockchain). On pourrait voir également la Blockchain et l'intelligence artificielle se rapprocher. Malheureusement, en l'état actuel des choses, la blockchain et le Big Data sont plutôt incompatibles (la blockchain n'étant ni prévue pour être rapide ni pour traiter de nombreuses données) de même pour les intelligences artificielles à apprentissage non supervisé qui requiert également beaucoup de données (en revanche rien n'empêche ces systèmes d'intelligence artificielle de créer ou gérer des blockchains).

La blockchain 2.0

L'autre voie, que j'appelle ici la blockchain 2.0, est l'évolution de la blockchain mais une évolution majeure ne remplace pas forcément la blockchain mais en fait une technologie similaire et plus évoluée à partir de celle-ci, un peu comme le BIOS et Windows ou la SOA (Service Oriented Architecture) et les micro-services, hors domaine numérique un peu comme les cabines téléphoniques et les smartphones. Cependant, prédire à quoi ressemblerait la blockchain 2.0 alors que nous ne sommes encore qu'au début de la blockchain, serait pure spéculation...

Arnaud Declochez (104 INA)

La blockchain pour les banques : une menace devenue une opportunité

La blockchain et les banques, le mariage impossible ?

Fin 2017, la valeur du bitcoin a dépassé le seuil des 16 000 dollars, provoquant une «ruée vers l'or» sur les cryptomonnaies, dont le bitcoin n'est que la plus connue. Les projets d'application de cette technologie blockchain (ou DLT pour Distributed Ledger Technology) se multipliaient à tous les secteurs, vantant encore une fois la désintermédiation, et les publicités incitaient les particuliers à investir massivement dans les cryptomonnaies. En 2019, Facebook a également sorti son projet de monnaie virtuelle Libra, basée sur une blockchain éponyme, reposant la question de l'impact de cette technologie sur le système monétaire et financier mondial.
Les banques ont tout d'abord été frileuses vis-à-vis de cette technologie. On pourrait résumer le bitcoin (et autre cryptomonnaies) à un logiciel et protocole de communication cryptée qui se substitue à la monnaie, à la Banque Centrale et à l'état qui l'encadre. Quand on comprend qu'une banque est avant tout un « tiers de confiance », devant satisfaire à de plus en plus de contrôles de conformité pour conserver leurs licences bancaires, on réalise alors que les cryptomonnaies prennent le contrepied total en proposant une organisation décentralisée, sans intermédiaire…et donc sans les banques (commerciales ou centrales) ni les contrôles qui vont avec. Cela explique que

les cryptomonnaies ont eu une réputation très sulfureuse, régulièrement associée au darkweb, blanchiment d'argent… C'est un frein important au mariage avec les banques, même si la maturité de la technologie apporte désormais certaines garanties (blockchain privées par exemple) et que les régulations se mettent en place.

De nombreuses applications prometteuses dans le milieu bancaire

Outre les cryptomonnaies, de nombreux projets ont émergé autour de cette technologie dans le milieu bancaire et qui peuvent apporter une réelle valeur ajoutée.

L'un de premiers cas d'usage est le transfert d'argent international. Particuliers et entreprises passent aujourd'hui par leur banque pour transférer des fonds moyennant un temps d'exécution (2-3 jours) et un coût (en moyenne des commissions de l'ordre de 7%), les banques s'appuyant elles-mêmes sur le réseau interbancaire SWIFT. Western Union est toujours le leader sur le marché, mais désormais des licornes type Ripple ou Stellar ont des belles réputations sur le marché.

Un autre cas d'usage qui intéresse fortement les banques concerne les métiers du Trade Finance et Supply Chain Finance : ces produits financiers (lettres de crédit, transactions « open account »,…) mettent en jeu de multiples acteurs (exportateur et sa banque, importateur et sa banque, douanes et autorités des ports, compagnie de fret,…), les échanges et signatures des documents nécessitant beaucoup de papiers et de contrôles au sein des équipes opérationnelles des banques. Les banques ont été à l'initiative du lancement d'initiatives comme Marco Polo, We.Trade, Contour et se sont organisées en consortium pour choisir les blockchains (technologies Corda et Hyperledger principalement) et mettre en place les gouvernances autour de ces outils. Les résultats sont prometteurs avec des premières transactions financières réalisées en 2019.

Passage de l'effet de mode à une solution industrielle

L'utilisation de la technologie blockchain au sein des banques se concrétise donc par des projets très concrets, avec des résultats encourageants…mais aussi un certain nombre d'obstacles sur la route :

- La performance à grande échelle (ou scalabilité) reste à prouver. Aujourd'hui, on peut effectuer une dizaine de transactions par seconde sur une blockchain, quand l'opérateur Visa en effectue 20 000 par seconde…L'impact environnemental de ces technologies est également un véritable problème, cette technologie étant gourmande en ressources matérielles informatiques.
- La protection des données est un autre élément clé : la sécurisation via des blockchains privées reste la piste privilégiée au niveau des acteurs, mais ne résout pas tous les problèmes. Comment supprimer certaines données pour être conforme aux lois GDPR, quand la blockchain fonctionne sur une base immuable, empêchant toute donnée d'être supprimée ?
- Enfin, les problématiques légales et règlementaires concernant les e-documents et e-signatures notamment sont un frein majeur à l'utilisation de la blockchain.

En conclusion, la blockchain ne sera pas une révolution mais peut apporter une réelle valeur ajoutée (gain pour les clients, réduction de risque ou de coût pour les banques) sur des cas d'usage spécifiques, beaucoup de travail restant à faire pour sécuriser son utilisation.

La blockchain, génératrice de confiance au service de l'homme : le cas Plastic Bank™

Christophe Chatelus (81 ILI)

Christophe Chatelus, IBM, architecte en systèmes d'information est en charge des relations avec les éditeurs de logiciel dans le secteur des services financiers.

A quoi ressemblerait notre vie de tous les jours si tout le monde se faisait totalement confiance ? Plus besoin de clés ou de codes pour fermer nos maisons, nos voitures. Plus besoin de coffres-forts, de contrats complexes à mettre en œuvre. Tout serait bien plus simple et irait bien plus vite.

Plus de confiance signifie plus d'efficacité

Un certain nombre de banques européennes par exemple, ont pris conscience que pour trouver de nouvelles opportunités de commerce, la première chose dont nous avions besoin était la confiance. La blockchain, grâce à ses caractéristiques d'inaltérabilité, de transparence et de traçabilité leur est apparue comme la seule technologie permettant d'augmenter la confiance et d'accélérer les échanges commerciaux. Aidées par IBM, dont je suis salarié, elles se sont constituées en consortium et ont créé un réseau à base de blockchain, qui a pris le nom de we.trade™.

La blockchain : confiance, transparence, efficacité bancaire

IBM a développé avec d'autres grandes entreprises des solutions autour de la blockchain, dans des industries très différentes, mais qui ont toutes ce point commun de la nécessité d'assurer un niveau de confiance que les techniques traditionnelles ne permettaient pas d'atteindre : la traçabilité alimentaire, avec Walmart (IBM Food Trust™), la traçabilité des transports de containers (Trade Lens™ avec

Maersk) ou encore les paiements internationaux (IBM World Wire™).
Les éditeurs de logiciels dans les Marchés Financiers, dont ma responsabilité consiste à les aider à développer et optimiser leurs produits sur nos solutions, m'ont rapidement fait mettre le pied à l'étrier de la blockchain il y a 5 ans maintenant. J'ai participé à un certain nombre de projets de par le monde, mais celui dont je souhaitais vous parler aujourd'hui, s'il n'est ni le plus médiatique, ni le plus générateur de retours financiers, gardera pour longtemps une place privilégiée dans mon parcours professionnel et ceci pour une raison : il allie intérêt d'une innovation technologique, caractère passionné des instigateurs du projet et altruisme, tant pour relever l'homme de la misère que de résoudre un immense problème environnemental rencontré par les pays en développement.

Plastic Bank en Haïti : la blockchain au service de l'homme et de la planète.

Il s'agit de Plastic Bank™, qui a choisi la Blockchain pour industrialiser une plateforme de recyclage de matières plastiques. Les rivières d'Haïti, regorgent de bouteilles en plastique. Ce plastique peut être recyclé par les industriels du domaine. Mais comment le ramasser ? L'idée de Plastic Bank est la suivante : des personnes ramassent ces bouteilles, les remettent à des centres de collecte qui inscrivent dans la blockchain le nom du collecteur, la quantité et la qualité du plastique apporté. En échange, le centre de collecte donnera des « jetons » virtuels. Ces derniers pourront être échangés contre des services fournis par des participants adhérant au projet : inscription de leurs enfants à l'école, fourniture d'aliments ou de services de santé. Le collecteur sera connu par un identifiant, se verra crédité de jetons en échange des plastiques qu'il aura rapportés. En résumé, en collaboration avec IBM et le fournisseur de services britannique Cognition Foundry™, Plastic Bank mobilise autour de la Blockchain des entrepreneurs de recyclage parmi les communautés les plus pauvres du monde pour nettoyer les déchets plastiques en échange de produits qui changent leur vie.

La confiance, assurée instantanément par la blockchain

La blockchain est utilisée pour suivre le cycle complet du plastique recyclé depuis la collecte, le crédit et la compensation jusqu'à la livraison aux entreprises pour réutilisation. L'intérêt essentiel de la technologie Blockchain ici est le renforcement de la confiance autour du système. Lorsque le collecteur apporte sa récolte au centre de collecte, ce dernier entre dans le système, par l'intermédiaire d'un simple smartphone, le nom du collecteur, la quantité et la qualité de matériel apporté. Ceci s'inscrit immédiatement dans la Blockchain et est accessible instantanément par tous les participants. Il suffit ensuite au collecteur de se rendre dans l'établissement fournisseur de service, qui saura, de façon certaine, combien de jetons possède l'interlocuteur qui se présentera, par exemple dans une école pour y inscrire son enfant.

En quoi la blockchain a-t-elle été nécessaire ?

Des technologies traditionnelles auraient pu être utilisées, mais cela aurait nécessité un audit régulier de Plastic Bank. Une base de données centralisée aurait pu être mise en œuvre pour distribuer les montants, mais elle aurait dû être ouverte à un contrôle minutieux, continuel et elle aurait dû être vérifiée par un tiers à l'échelle mondiale, ce qui aurait ralenti le processus et augmenté le risque de corruption. En effet, qui peut être garant que le nombre de jetons n'a pas été altéré ? Plastic Bank a voulu s'assurer que la majeure partie de l'argent était transférée entre les mains des pays en développement au lieu des mains d'intermédiaires. Grâce à la Blockchain, pas besoin de tiers de confiance et pas de possibilité de corruption. Le système repose sur confiance et transparence. Enfin, d'autres avantages couronnent le tout, par exemple rapidité et dématérialisation.

Sur quoi la solution repose-t-elle ?

La solution est basée sur Hyperledger Fabric, la blockchain imaginée par IBM et hébergée par le projet Open Source Hyperledger. J'ai eu la joie de participer au design de la solution Plastic Bank qui a été effectué par notre centre de compétence Blockchain IBM de Montpellier et développé par le partenaire britannique Cognition Foundry.

Et demain ?

Aujourd'hui, la solution, testée à Haïti, est passée en production dans ce même pays puis en Indonésie et aux Philippines. Le projet s'étend en ce moment à la Colombie et l'Egypte et enfin ce sera le tour de la Thaïlande et du Vietnam dans les mois qui viennent.
Ce n'est pas si fréquent de pouvoir combiner dans le milieu professionnel : rentabilité d'un projet, protection de la planète, développement de la classe sociale la moins favorisée de pays en développement et découverte d'une technologie tout à fait innovante et prometteuse. Voilà bien un projet qui me semble entrer dans la perspective pédagogique de l'ingénieur Icam : ouverture au monde, solidarité et excellence technique.

Bitcoin et blockchain : une révolution inéluctable

François Miquel (103 ITO)

De la banque au bitcoin

Diplômé de l'Icam Toulouse en 2003, j'ai rapidement intégré un cabinet de conseil dans le secteur bancaire où je me suis investi 14 ans durant. Je suis tombé dans le Bitcoin en 2015 comme Alice dans le terrier du lapin blanc : un sujet à la croisée des sciences informatiques et économiques. C'est donc en octobre 2018, portés par la passion, que mon associé Baptiste Lac et moi, nous nous sommes lancés dans l'entreprenariat et nous avons ouvert le Comptoir des Cybermonnaies au cœur de Bordeaux. C'est à la fois un bureau de change qui permet l'achat et la revente de cryptomonnaies contre euros et un organisme de formations dédiées à Bitcoin et aux protocoles à blockchain.

Des origines de la blockchain

Contrairement à une idée largement répandue dans les médias, le concept de blockchain est bien antérieur à la création de bitcoin. C'est en 1991 qu'il voit le jour pour un système d'horodatage. L'idée est d'utiliser le journal du New York Times tiré à plusieurs centaines de milliers d'exemplaires pour y publier l'empreinte de documents numériques. Les fonctions cryptographiques permettent de produire le hash (une chaîne de caractères alphanumériques) de tout document numérique. A l'instar d'une empreinte digitale, il est unique pour chaque objet numérique distinct et permet de l'identifier avec certitude. Le quotidien tient lieu de registre distribué et son grand tirage dissuade toute tentative d'antidater les documents horodatés, car cela nécessiterait de remplacer tous les exemplaires distribués par une version falsifiée.

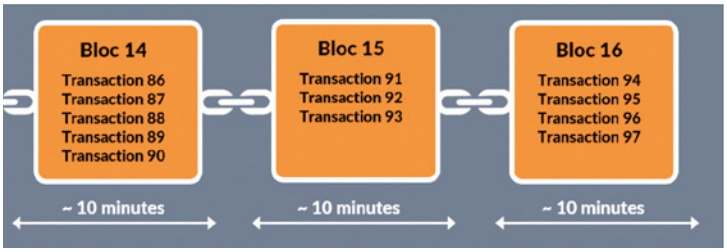
Bitcoin ou blockchain renaissance

Début 2009 voit l'avènement de Bitcoin : un protocole informatique, un réseau décentralisé et une unité de compte. Une transaction Bitcoin permet de transférer les jetons numériques entre utilisateurs du réseau, sans l'intervention de tiers de confiance, tout en respectant les règles du protocole. Toutes les 10 minutes environ est créé un nouveau bloc contenant les dernières transactions et

Le Comptoir des Cybermonnaies

lié au bloc précédent. Les transactions sont donc structurées en une chaîne de blocs que l'on peut voir comme un grand livre de compte unique, public, infalsifiable et dupliqué sur l'ensemble des nœuds du réseau : la blockchain !

Représentation d'une blockchain



Une innovation numérique majeure

Bitcoin permet pour la première fois de transférer un objet numérique unique, de pair à pair, sans intermédiaire, et sans le dupliquer. Pour cette raison souvent mal perçue il s'agit d'une révolution numérique majeure comparable à Internet.

La tokenisation ou la numérisation des actifs

Certes, Bitcoin revendique les fonctions d'une monnaie : stockage de valeur, medium d'échange et unité de compte. Mais il ouvre également la voie à la numérisation des titres et actifs financiers, des biens immobiliers, des brevets et droits d'auteurs en les associant à des jetons. C'est le processus de tokenisation.

L'horodatage ou la certification des documents

Par ailleurs une empreinte numérique peut être insérée dans chaque transaction, conférant à Bitcoin la propriété d'horodatage. Les cas d'usage sont nombreux, de la certification du diplôme (Ordre des Experts Comptables) à la traçabilité et la logistique des produits (Walmart sur des produits alimentaires. Everledger pour la certification de diamants).

Le smart contract ou l'automatisation des contrats

Enfin il convient de préciser que les transactions sont programmables. Elles intègrent des scripts (lignes de codes). Cela permet de conditionner l'exécution d'une transaction à une durée ou à un événement. Sur ce principe s'est développé le concept du smart contract: un programme inscrit dans la blockchain, dont les instructions s'exécutent automatiquement et conduisent selon certaines conditions à transférer ou stocker de la valeur. Un concept très prometteur pour l'ingénierie financière des secteurs banque / assurance.

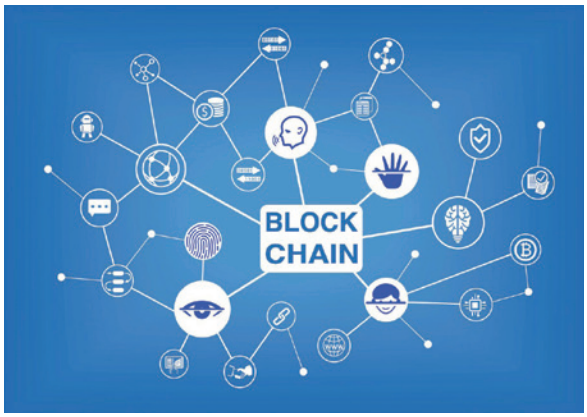
Un outil au service de la société

Dans une vision occidentalo-centrée, Bitcoin est perçu au mieux comme un gadget et au pire comme un actif hyper-spéculatif. Pourtant plus d'un adulte sur trois dans le monde est non bancarisé, principalement dans l'hémisphère sud. Or, Bitcoin est sans frontière, sans permission et incensurable. Les cryptomonnaies au service de l'inclusion bancaire dans le monde est un argument tellement évident et louable que Facebook n'a pas hésité à le reprendre à son compte pour le projet de création de sa propre crypto-monnaie : le Libra. Gageons que le grand public ne sera pas dupe de ce discours marketing mais qu'il s'appropriera les cryptomonnaies comme il l'a fait avec Internet.

La blockchain : un progrès ?

Denis Peccoud (100 ILI)

2007, les banques ne maîtrisent plus la qualité de leurs actifs. L'appât du gain a fait circuler des dettes aussi opaques qu'irresponsables. Des millions de familles s'enfoncent dans la pauvreté. La bulle des produits dérivés, impossible à quantifier, amplifie la déroute. Les banques se protègent en se coupant des autres banques. Elles accélèrent la panique… et les faillites.



Le « plus jamais ça ! » motive alors l'innovation mathématique et informatique. Ainsi naissent en 2008 la blockchain et son premier usage, le bitcoin.

Mon métier étant de transformer des banques pour BNP Paribas, la blockchain est un sujet important de mon quotidien. L'objectif de cet article est de partager avec vous l'état de mes réflexions, sans aborder les aspects techniques dont je ne suis pas expert.

La blockchain pour les nuls

La Blockchain permet d'écrire et de certifier une transaction entre deux parties dans un registre partagé. Chaque partie peut consulter ce registre sans modifier les entrées précédentes. Ce registre n'est pas détenu par un serveur central mais par tous les ordinateurs des membres de la chaîne (base de données distribuée). Difficilement corruptible, la blockchain assure donc le stockage et l'échange d'informations sensibles sans l'intervention d'un tiers de confiance.

Une révolution technologique à maîtriser

Par ses attributs, la blockchain transforme trois grandes fonctions.

- Le transfert de valeur : plus besoin des banques, de notaires, d'Etat etc… pour garantir les transactions entre personnes. La blockchain offre une solution totalement décentralisée et plus sécurisée. Les crypto monnaies en sont une illustration.
- La totale traçabilité de la blockchain peut être utilisée par les chaînes logistiques, pour la certification des diplômes, pour garantir l'historique des termes et conditions d'un contrat, pour développer les identités numériques... A terme, un EURO pourrait même contenir son histoire, ce qui permettrait une lutte totale contre le crime financier ou écologique.
- L'automatisation de l'exécution des contrats sous forme de « Smart Contracts » est accélérée. Ces contrats sont comme des macros Excel partagées entre des parties contractantes. Ils permettent de gérer le paiement de prime d'assurances, un processus complexe de commerce international, etc…

Ces usages sont réels même si encore balbutiants. Ils se développent lentement car ils nécessitent une adaptation des cadres réglementaires, des techniques de financement etc… Cependant, il est fortement probable que la blockchain sera un standard dans les années à venir.

Principale limite technologique, son efficience

De par sa logique distribuée, la technologie est aujourd'hui énergivore et assez « lente ».

Par exemple, le bitcoin traite maximum 7 transactions par seconde, alors qu'un réseau comme VISA peut en traiter 45 000. Et, pour ce faire, le réseau bitcoin consomme autant d'énergie qu'un pays comme le Maroc.

Une idéologie libertaire sous-jacente dangereuse

Les blockchain peuvent être « privées » ou « publiques ». Les blockchain privées ont un certain niveau de gouvernance : par un contrat commercial, par des niveaux de permissions, par un accès restreint à certains participants…

Dans la blockchain publique, la gouvernance est totalement décentralisée, ouverte et appartient aux membres du réseau. Cette gouvernance peut être vertueuse : par exemple pour assurer un cadastre transparent dans une société corrompue.

Néanmoins, dans la plupart des cas, il s'agit d'un crypto-anarchisme.

L'idée fondatrice est de ne plus faire confiance à des tiers. OK pour se passer des banquiers, même si cela ne m'arrange pas ! Mais nos institutions n'ont-elles aucune valeur ? Qu'est-ce qu'une devise sans une politique monétaire ? La somme d'intérêts individuels vaut-elle projet collectif ?

Le mensonge de cette idéologie est ce qui me choque le plus. Le pouvoir est finalement remis dans la capacité de calcul qui, comme la richesse, se concentre. La sécurité d'une blockchain repose sur le fait qu'aucun membre du réseau ne dépasse 51% de la capacité de calcul. Or la Chine possède déjà 70% de la capacité de calcul du réseau bitcoin, Google et IBM investissent le Quantum Computing…

Les réseaux sociaux ont affaibli nos démocraties. Une utilisation libertaire de la blockchain construira un colosse aux pieds d'argile.

A quand la chain humaine qui fait block pour un monde meilleur ?

La blockchain, le numérique et leurs impacts sur la consommation énergétique mondiale

Article transmis par Nicolas Pot (76 ILI)

Dans son livre « L'Intelligence artificielle n'existe pas », Luc Julia, cocréateur de l'assistant vocal Siri, interpelle à propos des impacts énormes du développement du numérique sur la consommation énergétique mondiale. Voici quelques extraits de son livre[1] :

« Toutes les études arrivent à la même conclusion : Autour de 2020, l'économie digitale qui regroupe Internet, les terminaux, les réseaux, les cryptomonnaies, la technologie blockchain et les centres de stockage pèsera pour 20 % dans la consommation électrique de la planète bleue… On estime qu'un internaute moyen consomme 365 kWh d'électricité pour son activité en ligne et 2900 litres d'eau par an. Pour vous donner une idée ça donne la consommation annuelle électrique de 10 Haïtiens, et assez d'eau pour survivre pendant deux ans et demi ».

« Chaque photo que vous postez sur votre mur Facebook consomme à elle seule autant que trois ou quatre ampoules basse consommation de 20 watts allumées pendant une heure ! Sans compter qu'il faut ensuite les stocker sur les serveurs et bien les refroidir... Une transaction de la blockchain est estimée consommer 767 kWh, alors qu'une transaction par carte Visa utilise moins de 2Wh ».

« Il est donc important de chercher des solutions qui fonctionneraient plus comme notre cerveau humain c'est-à-dire en utilisant beaucoup moins d'énergie. DeepMind consomme plus de 440 000 watts par heure juste pour jouer au go, alors que notre cerveau fonctionne avec seulement 20 watts par heure pour effectuer bien d'autres tâches ».

« À l'avenir, au lieu de continuer dans la voie du big data, il faudrait se tourner vers le small data qui consommerait beaucoup moins d'énergie. Nous ne savons pas encore comment, mais grâce à la multimodalité[2] et à la diversité des sources je suis persuadé que nous ferons d'énormes progrès dans les années qui viennent. Avec le small data il va falloir modifier les algorithmes, changer de méthodes et de stratégies, tout en obtenant des résultats similaires. Il y a beaucoup de recherches et de travail à faire pour y arriver, ce n'est pas très à la mode aujourd'hui, parce que les méthodes basées sur le big data marchent bien et permettent d'avoir des résultats impressionnants, mais cette solution de facilité va bientôt montrer ses limites ».

« Dans les soixante dernières années, les technologies dérivées de l'IA nous ont apporté un plus grand confort de vie, ont favorisé la croissance économique, et ont parfois même faire reculer les guerres, la famille et les épidémies. Je pense également que nous trouverons des solutions pour réduire son impact écologique. »

[1] **Luc Julia « L'Intelligence artificielle n'existe pas » -First Editions- Janvier 2019**

[2] **NDLR : la multimodalité au sens sémiotique, désigne la mise en œuvre dans la production du sens de divers modes d'expressions combinés, tels la parole, la gestuelle, les images fixes ou animées et un accompagnement sonore.**

« Icam à Vie » offre une initiation à la technologie de la blockchain

Un parcours certifiant a été créé. Le certificat est donné pour ceux qui ont suivi avec succès les deux cours suivants : « décrypter la technologie blockchain » et « découvrir les applications de la technologie blockchain ».

Le premier cours permet de maîtriser les bases, de définir les principales notions : consensus, minage, smart contracts et de comprendre les mécanismes de réplication et de distribution du registre. Trois niveaux sont proposés : base, avancé et coach. Huit alumni ont atteint le niveau coach. Il faut compter environ une heure pour y arriver.

Le second cours illustre en deux niveaux (base et avancé) les domaines d'applications de la technologie blockchain : les plus connues banques et assurances, mais aussi la musique, l'énergie , le médical et la santé. Il décrit les blockchains existantes les plus utilisées : Bitcoin, Ethereum, Hyperledger fabric . Enfin pour terminer, les limitations de la technologie sont décrites. Une dizaine d'alumni ont réussi les deux niveaux. Il faut compter une demi-heure pour les compléter.

Par ailleurs pour ceux qui sont pressés, ces cours ont été fractionnés en une quinzaine de micro-learnings qui nécessitent de 5 à 10 minutes d'attention.

De plus un groupe de discussion a été créé dans LinkedIn. Son intitulé est « Icam à Vie blockchain » et son adresse : linkedin.com/groups/12371274.

Rendez-vous donc sur la plateforme d'e-learning d'Icam à Vie, si vous voulez acquérir les premières notions de cette nouvelle technologie. C'est un bon outil de vulgarisation à la portée de tous.

Jean-Yves Aubé (70 ILI)