LA RÉVOLUTION « BLOCKCHAIN » (CHAÎNE DE BLOCS)

Une innovation technologique majeure ?

Véronique Pelletier
veronique.pelletier@adeli.org

Résumé :

Cet article permet d'avoir une première idée de ce qu'est la blockchain. Il développe l'explication de l'une de ses applications à travers la monnaie « bitcoin ». Il indique enfin des articles et ouvrages pour approfondir le sujet.

Mots-clés :

Blockchain, système distribué, archivage

Parmi les innovations technologiques de ces dernières années, les bases de données distribuées, le peer to peer, la blockchain, la cryptologie sont des nouveautés dont on parle beaucoup. Essayons de les décrypter…

INNOVATION

Qu'est-ce que l'innovation ? Voici deux définitions :

Cité des sciences

« Innover, c'est réussir le pari de lancer quelque chose de nouveau sur le marché, une source d'énergie, une matière première, un produit ou un service, un mode d'organisation ou un procédé. Il y a mille exemples d'innovations mais pas de définition standard. »

Wikipédia

« Comprendre le concept d'innovation implique que l'on distingue bien le résultat concret (produit, service, procédé, etc.) de l'action d'innover, du processus abstrait qui permet de les réaliser.

Sur le plan individuel, l'innovation est le fait de rompre avec ses habitudes, de faire quelque chose pour la première fois ou d'être le premier à le faire créativement. Elle se rapproche en cela de la créativité. »

LA TECHNOLOGIE « BLOCKCHAIN »

La « blockchain » est une technologie innovante. Elle a fait couler beaucoup d'encre en 2016.

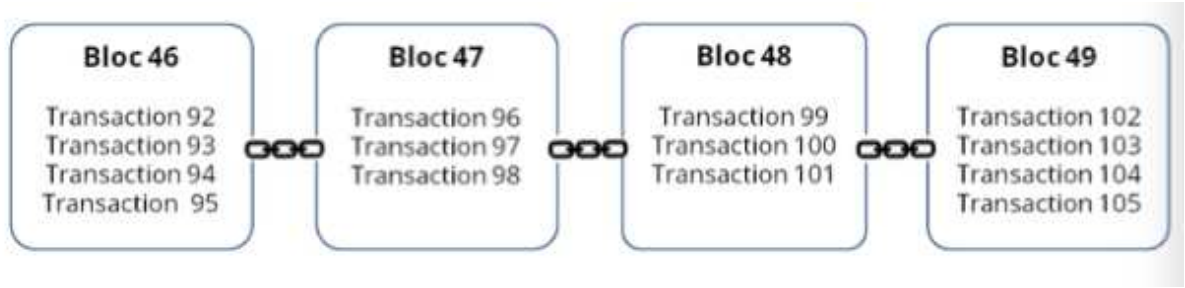
Le mot « Blockchain » peut se traduire, en français, par chaîne de blocs. Il s'agit d'un système de validation fiable, distribué, coûteux en ressources.

DÉFINITIONS ET FONCTIONNEMENT

De Blockchain France[1]

« "La « blockchain » est une technologie de stockage et de transmission d'informations transparentes, sécurisées et fonctionnant sans organe central de contrôle.

Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée. Elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. »



Wikipédia

« La chaîne de blocs (blockchain) est une forme de mise en œuvre de la solution du problème des généraux byzantins, métaphore qui traite de remise en cause de la fiabilité des transmissions et de l'intégrité des interlocuteurs. La question est de savoir comment prendre en compte une information dont la source ou le canal d'information est suspect. La solution implique l'établissement d'un algorithme (d'une stratégie) adapté. Ce problème a été traité en profondeur pour la première fois dans l'article The Byzantine Generals Problem publié en 1982. »

LE BITCOIN

Le Bitcoin est la crypto-monnaie[2] la plus utilisée, qui se fonde sur la technologie Blockchain.

Ce qu'en disent les organisateurs

Le Bitcoin est un réseau de paiement novateur et une nouvelle forme d'argent.

C'est la première devise monétaire électronique décentralisée.

Les bitcoins sont des jetons électroniques que vous pouvez envoyer sur Internet.

[1] Blockchain France est une entreprise française créée en 2015.
[2] D'après wikipedia, une crypto-monnaie ou **monnaie** cryptographique est une **monnaie** électronique sur un réseau informatique pair à pair ou décentralisée basé sur les principes de la **cryptographie** pour valider les transactions et émettre la **monnaie** elle-même

Les bitcoins se transmettent d'une personne à une autre à travers le réseau sans passer par une banque ou une chambre de compensation.

Cela signifie que les frais de transaction sont beaucoup plus bas, vous pouvez les utiliser dans n'importe quel pays, votre compte ne peut pas être bloqué et il n'y a pas de conditions préalables ou de limites arbitraires.

Comment cela fonctionne-t-il ?

Plusieurs bourses de change existent où vous pouvez échanger vos bitcoins contre des Dollars, des Euros ou des Yens.

Vos bitcoins sont conservés dans votre portefeuille électronique sur votre ordinateur ou votre téléphone mobile.

Envoyer des bitcoins est aussi simple que d'envoyer un e-mail et vous pouvez acheter n'importe quel article ou service avec des bitcoins.

Le réseau Bitcoin est sécurisé par des personnes que l'on nomme les mineurs (métaphore des chercheurs d'or).

Les mineurs sont récompensés avec des bitcoins nouvellement créés pour vérifier les transactions. Aujourd'hui, la valeur de la récompense est de 25 B, soit environ 9 000 €. Un Bitcoin valant 365 € aujourd'hui. Les Mineurs mettent la puissance de leur ordinateur au service de la communauté.

Lorsque les transactions sont vérifiées, elles sont enregistrées dans un registre transparent et public, répliqué.

Bitcoin ouvre la porte à une nouvelle plateforme pour l'innovation. C'est de l' « open innovation ».

Le logiciel est entièrement libre et tout le monde peut consulter et modifier le code.

Bitcoin change le monde de la Finance de la même façon que le Web a changé le monde de l'Édition. Les grandes banques, les grands assureurs se forment à ces technologies.

Quand tout le monde a accès à un marché global, de nouvelles idées porteuses d'innovation peuvent apparaître.

Bitcoin est un très bon moyen pour réduire les frais de transaction des entreprises. C'est une technologie pair à pair (peer to peer – p2p) fonctionnant sans autorité centrale.

Le système fonctionne parce que de nombreux utilisateurs utilisent le logiciel et communiquent via un logiciel peer-to-peer (p2p). Est-ce encore expérimental ?

Satoshi Nakamoto

Le Bitcoin a été inventé par Satoshi Nakamoto, japonais qui vit en Californie. C'est un homme doté de compétences fortes en mathématiques, en informatique et en ingénierie. Il est secret. Il n'aime pas les banques. Il possède la plus grande fortune en monnaie numérique au monde (environ 400 millions de dollars). Des bruits courrent sur le fait qu'il s'agissait en fait d'un projet secret de Samsung, Toshiba, Nakamichi, Motorola.

LA RÉVOLUTION BLOCKCHAIN

Philippe Rodriguez a écrit « *La révolution Blockchain Algorithmes ou institutions, à qui donnerez-vous votre confiance ?* », un livre tout à fait passionnant publié aux éditions Dunod.

« Sur le plan technique, la blockchain fonctionne comme un vaste registre public, intégrant l'ensemble des transactions validées dans une liste sans fin. Ce registre fait donc figure d'historique

de toutes les transactions menées par tous les utilisateurs depuis le début de la constitution du réseau. » Il n'est pas possible de modifier ces transactions.

« Pour fonctionner, la blockchain a besoin d'une capacité énorme de calcul et mobilise donc un réseau d'ordinateurs distribués ».

Cette innovation technologique a été développée par des communautés de mathématiciens et d'informaticiens à la fin des années 1990 et au début des années 2000.

Philippe Rodriguez commence son livre par cette citation :

> *« Vous ne changerez jamais les choses en vous battant contre la réalité existante. Pour véritablement changer votre environnement, construisez un nouveau modèle qui rend obsolète le modèle existant. » Richard Buckminster Fuller, 1982*

Sommes-nous à l'aube d'une véritable révolution ?

The Big Block Theory

Le 3 avril 2017, à l'ESCP Europe, j'ai participé à un séminaire « The Big Block Theory ».

Pour Primavera Filippi, c'est une « collaboration pour générer de la valeur » : une « production participative ».

Sajida Zouarhi, d'Orange Lab a expliqué comment redonner à l'utilisateur le contrôle de ses données. Les données critiques (de crise, personnelles, métier, bancaire, d'alerte, médicales...) doivent être maîtrisées. Elle nous a parlé de vision de bout en bout, de consentement (la donnée peut ne pas être accessible dans une fenêtre de temps).

Sébastien Choukroun de Pwc France[3] nous a parlé de la théorie des jeux à champ moyen, stratégie optimale, de la théorie des jeux stochastiques (on peut se ramener à deux groupes de joueurs) et de la mise en place de consortiums[4].

Pour Nicolas Herbant du LaBRI[5] de Bordeaux, la blockchain est un vecteur de confiance à la collaboration numérique.

Christine Hennebert du CEA Grenoble cherche à savoir si la consommation d'énergie est acceptable.

Simon Janin de l'école polytechnique de Zürich a expliqué le fonctionnement dans la blockchain de l'échange d'un fichier entre deux personnes, en rémunérant l'émetteur et prouvant la fiabilité de l'échange.

Loren Jolly, doctorante en droit pénal au Luxembourg, travaille sur la prévention de la criminalité et à une réglementation pénale commune à la commission européenne. Avec la blockchain, une unité de monnaie n'est utilisée qu'une seule fois. Elle nous parle du principe de proportionnalité, du droit fondamental à la protection des données personnelles. La blockchain conserve toutes les transactions.

Axel Moinet termine sa thèse à Dijon. En 2016, on compte 6,4 milliards d'objets connectés dans le monde, dont 52% n'ont aucune mesure de sécurité. Comment identifier un device ? Comment lui faire confiance ? Où stocker l'information ? Il travaille sur la confiance entre humains. Il se réfère au HKT : Human–Like Knowledge-based Test. Les blocks ont un identifiant unique. On peut retrouver ses actions passées sur la blockchain. C'est une base de données distribuée, sûre et inaltérable.

Thomas Sibut-Pinote termine sa thèse à Polytechnique sur le plateau de Saclay. Il travaille sur la preuve formelle. Un algorithme de consensus appliqué à la répartition des jetons ayant une valeur

[3] http://www.pwc.fr/
[4] Le consortium est un type de blockchain intermédiaire entre la blockchain privée et la blockchain publique
[5] Laboratoire bordelais de recherche en informatique : *https://www.labri.fr/*

monétaire. Les smart contracts sont visibles par tout le monde. Dans l'industrie, 1000 lignes de code génèrent 15 à 20 bugs. Le code source est public et non modifiable. C'est un environnement en mémoire partagée avec d'autres programmes. Il faut spécifier les programmes, écrire leur code, vérifier par les méthodes formelles. Il travaille sur la blockchain tezos créée par Arthur Breitman. Il parle de Proof of work, de proof of stake, de contrat multisig (signature), du langage fonctionnel oCaml, de problème de gouvernance.

1er forum parlementaire

Le 1er forum parlementaire sur la blockchain s'est tenu le 4 octobre 2016. Il était animé par Daniel Jarjoura, fondateur et CEO de STUDIIO qui a déclaré :

« Avec près de $500M investis dans les startups blockchain et des premiers produits annoncés par des géants du secteur comme IBM, Microsoft ou encore Accenture, les impacts industriels de cette technologie de gestion de transactions ne sont encore qu'à leurs prémisses. Il serait pourtant dommage de ne considérer la blockchain que comme une simple nouvelle technologie. »

Cet événement était parrainé par deux parlementaires : Laure de la Raudière (LR), députée d'Eure-et-Loir et Jean Launay (PS), député du Lot.

CONCLUSION

Au fil de mes lectures, j'ai pu me faire une idée de l'intérêt de la blockchain. Cela me semble une innovation technologique majeure, en ce sens qu'il s'agit d'une mise en relation de personnes entre elles, sans nécessité d'un tiers de confiance. Cette initiative est issue du peer to peer et de la mise à disposition de titres de musique entre les personnes. Les plateformes et la technologie le permettent, tandis que les citoyens veulent une société plus fluide. Ceux-ci ne souhaitent plus une hyperadministration toute-puissante…

Bien sûr, il faut aussi réfléchir en termes d'environnement, que je n'ai pas pu détailler, dans le cadre de ce bref article, dans tous ses aspects, mais un consensus décentralisé peut s'installer par ce moyen sur la véracité des transactions. De puissants calculs sont effectués. Un outil de cryptographie asymétrique est utilisé. Un algorithme de hachage permet de vérifier l'intégrité des documents. La preuve de travail (proof of work) est encore un outil utilisé : c'est une énigme mathématique complexe à résoudre.

The Dao - *Decentrazed autonomous organization* (Organisation autonome décentralisée) est un fonds d'investissement participatif décentralisé sur la blockchain ethereum. Sa crypto-monnaie est l'ether. Une faille de The Dao a permis de subtiliser l'équivalent de 50 millions d'euros. Mais, le vol a été bloqué par un « *hard fork* » de la blockchain (une deuxième branche a été créée). Il nous faudra encore un peu de temps pour nous en convaincre…

Encore un peu de travail est nécessaire pour obtenir ma confiance…

Dans son livre « *La quatrième révolution industrielle* », Klaus Schwab présente le couple formé par « le bitcoin et la blockchain » comme l'une des 23 mutations les plus profondes en cours. Le point de bascule devrait être atteint lorsque 10% du PIB mondial sera stocké sur une technologie de blockchain. Il cite des impacts positifs, mais aucun impact négatif, ce qui n'est pas le cas de la plupart des autres mutations présentées.

Aucun impact négatif ? Pour la petite histoire, le bitcoin aurait aussi été utilisé, selon certaines rumeurs, par des réseaux terroristes ou maffieux, et pour du blanchiment d'argent... La sécurité doit évoluer.

RÉFÉRENCES

- http://www.01net.com/actualites/on-a-retrouve-satoshi-nakamoto-le-createur-de-bitcoin-615462.html
- https://bitcoin.org/fr/
- weusebitcoins.com
- http://www.01net.com/actualites/on-a-retrouve-satoshi-nakamoto-le-createur-de-bitcoin-615462.html
- http://www.cite-sciences.fr/archives/francais/ala_cite/expositions/observatoire-innovations/definition-innovation/index.html
- http://lentreprise.lexpress.fr/high-tech-innovation/les-dix-innovations-technologiques-les-plus-prometteuses-du-monde-en-2016_1757510.html
- https://blockchainfrance.net/2016/03/04/comprendre-ethereum/
- https://blockchainfrance.net/2015/10/24/la-france-ne-doit-pas-rater-la-revolution-blockchain/
- https://h2.university/magazine/l-attaque-de-thedao-etape-par-etape
- http://www.france24.com/fr/20160519-dao-fonds-investissement-record-blockchain-ether-ethereum-dao-bitcoin-monnaie-slock-uber
- https://www.contrepoints.org/2016/11/15/271038-entretien-arthur-breitman-projet-de-blockchain-tezos